

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Kunio Kobayashi et al.

Serial No.: To be assigned

Art Unit: To be assigned

Filed: Herewith

Examiner: To be assigned

For: SYSTEM AND METHOD FOR
QUANTITATIVE COMPETITION
AND RECORDING MEDIUM
HAVING RECORDED THEREON
PROGRAM FOR IMPLEMENTING
THEM

Atty Docket: 0162/00561

**SUBMISSION OF CERTIFIED PRIORITY DOCUMENT(S) and
CLAIM TO PRIORITY UNDER 35 U.S.C. § 119**

Commissioner for Patents
Washington, D.C. 20231

Sir:

Priority under 35 U.S.C. § 119 is hereby claimed to the following priority document(s), certified copies of which are enclosed. The documents were filed in a foreign country within the proper statutory period prior to the filing of the above-referenced United States patent application.

<u>Priority Document Serial No.</u>	<u>Country</u>	<u>Filing Date</u>
205004/99	Japan	July 19, 1999
247060/99	Japan	September 1, 1999
2000-016020	Japan	January 25, 2000
2000-047323	Japan	February 24, 2000

Acknowledgement of this claim and submission in the next official communication is respectfully requested.

Respectfully submitted,

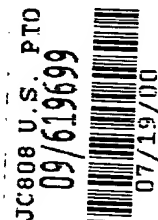


Morris Liss, Reg. No. 24,510
Pollock, Vande Sande & Amernick
1990 M Street, N.W.
Washington, D.C. 20036-3425
Telephone: 202-331-7111

Date: July 19, 2000



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 9 年 7 月 1 9 日

出 願 番 号

Application Number:

平成 1 1 年特許願第 2 0 5 0 0 4 号

出 願 人

Applicant (s):

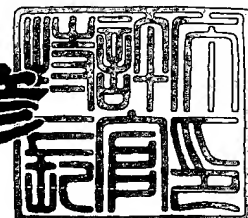
日本電信電話株式会社



2 0 0 0 年 6 月 2 3 日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特 2 0 0 0 - 3 0 4 6 8 3 5

【書類名】 特許願

【整理番号】 NTTH115596

【提出日】 平成11年 7月19日

【あて先】 特許庁長官殿

【国際特許分類】 G09C

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 小林 邦生

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 森田 光

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子競争入札方法、その装置及びプログラム記録媒体

【特許請求の範囲】

【請求項 1】 複数の入札装置から、入札価格と、その入札装置を特定する識別子とを開札装置へ送り、開札装置で受信した入札価格中の最大値又は最小値を落札価格とし、その落札価格とその入札価格を提示した入札装置の識別子を出力する電子競争入札方法において、

入札装置は入札価格を一方向性関数を用いて整数の入札指標に変換して、開札装置へ送り、

開札装置は各受信した入札指標から、非落札価格を全入札装置に知られることなく、最大入札価格又は最小入札価格を落札価格として決定することを特徴とする電子競争入札方法。

【請求項 2】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) の上記入札指標を

$$r_i = g(h^{f(PR_i)}(IV_i))$$

とし、 g は一方向性関数を、 IV_i は入札装置 i に固有の初期値、 $f(PR_i)$ は入札装置 i の入札価格 PR_i の関数であり、 PR_i が大きくなる程大きな正の整数値を出力する関数である、 $h^{f(PR_i)}$ は IV_i に対して一方向性関数 h を $f(PR_i)$ 回繰返すことを示し、

各入札装置 i は $C_i = h^{f(n+1)}(IV_i)$ (n は入札価格の上限値) を共有記録媒体に記録して全入札装置に公開していることを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 3】 開札装置での落札価格の決定は、

処理パラメータ k を上限値 n に設定する過程と、

$\delta_i = g(h^{f(k)}(IV_i))$ を各 IV_i について演算する δ_i 演算過程と、

δ_i が入札指標 r_i と一致するか調べる照合過程と、

上記照合過程で何れの IV_i についても一致するものがなければ上記 k を -1 して上記 δ_i 演算過程に戻る過程と、

上記照合過程で一致すると、その時の k を落札価格とし、その一致した r_i と

対応する識別子 ID_i とを出力する過程とにより行われることを特徴とする請求項 2 記載の電子競争入札方法。

【請求項 4】 開札装置に受信した各入札価格 PR_i と識別子 ID_i を、何れの装置からも参照可能な共有記録媒体に記録し、

上記落札価格 k と識別子 ID_i とに対する $h^{f(k)}(IV_i)$ をも出力することを特徴とする請求項 3 記載の電子競争入札方法。

【請求項 5】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) の上記入札指標を、

$$r_i = g(h^{f(n, PR_i)}(IV_i))$$

とし、 g は一方向性関数、 IV_i は入札装置 i に固有の初期値、 PR_i は入札装置 i の入札価格、 n は入札価格の上限値、 $f(n, PR_i)$ は PR_i が大きくなる程、小さな正の整数値を出力する関数、 $h^{f(n, PR_i)}$ は IV_i に対して一方向性関数 h を $f(n, PR_i)$ 回繰返すことを示し、

各入札装置 i は $C_i = h^{f(n, q-1)}(IV_i)$ (q は入札価格の下限值) を共有記録媒体に記録して全入札装置に公開していることを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 6】 開札装置での落札価格の決定は、

処理パラメータ k を下限値 q に設定する過程と、

$\delta_i = g(h^{f(n, k)}(IV_i))$ を各 IV_i について演算する δ_i 演算過程と

δ_i が入札指標 r_i と一致するか調べる照合過程と、

上記照合過程で何れの IV_i についても一致するものがなければ上記 k を +1 して上記 δ_i 演算過程に戻る過程と、

上記照合過程で一致すると、その時の k を落札価格とし、その一致した r_i と対応する識別子 ID_i とを出力する過程とにより行われることを特徴とする請求項 5 記載の電子競争入札方法。

【請求項 7】 開札装置に受信した各入札価格 PR_i と識別子 ID_i を、何れの装置からも参照可能な共有記録媒体に記録し、

上記落札価格 k と識別子 ID_i と対応する $h^{f(n, k)}(IV_i)$ をも出力するこ

とを特徴とする請求項 6 記載の電子競争入札方法。

【請求項 8】 開札装置に入力された複数の入札指標 r_i 、識別子 ID_i を共有記録媒体に蓄積する過程と、

パラメータ k と n をセットする過程と、

全入札装置 i に $h^{f(k)}(IV_i)$ の提示を要求する提示要求過程と、

その提示要求を受けた入札装置 i はその初期値 IV_i を用いて $h^{f(k)}(IV_i)$ ($=D_i$) を生成して開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する過程と、

これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の対応する C_i と各々一致するかを検証する過程と、

その検証で全て一致すると、 $g(D_i)$ を生成する過程と、

その各 $g(D_i)$ が共有記録媒体上の入札指標 r_i に一致するかを検証する過程と、

その検証で r_i と一致するものが 1 つもなければ、共有記録媒体上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し、 k を -1 して上記提示要求過程に戻る過程と、

上記検証で r_i と一致するものがあればその時の k を落札価格とし、その k と、この落札価格を提示した入札装置の識別子 ID_i を出力する過程とを有することを特徴とする請求項 2 記載の電子競争入札方法。

【請求項 9】 開札装置に入力された複数の入札指標 r_i 、識別子 ID_i を共有記録媒体に蓄積する過程と、

パラメータ k を下限値 q にセットする過程と、

全入札装置 i に $h^{f(n,k)}(IV_i)$ の提示を要求する提示要求過程と、

その提示要求を受けた入札装置 i はその初期値 IV_i を用いて $h^{f(n,k)}(IV_i)$ ($=D_i$) を生成し、この D_i を開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

全 D_i に対して、 $h^{f(n,q-1)-f(n,k)}(D_i)$ を作成する過程と、

これら $h^{f(n,q-1)-f(n,k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する過程と、

その検証で全て一致すると、 $g(D_i)$ を生成する過程と、

その各 $g(D_i)$ が共有記録媒体上の入札指標 r_i に一致するかを検証する過程と、

その検証で r_i と一致するものが 1 つもなければ、共有記録媒体上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し、

k を + 1 して上記提示要求過程に戻る過程と、

上記検証で r_i と一致するものがあればその時の k を落札価格とし、その k と、一致した r_i と対応する入札装置の識別子 ID_i とを出力する過程とを有することを特徴とする請求項 5 記載の電子競争入札方法。

【請求項 10】 開札装置に入力された複数の入札指標 r_i 、識別子 ID_i を共有記録媒体に蓄積する過程と、

パラメータ k を上限値 n にセットする過程と、

全入札装置 i に価格 k で入札したかどうか質問する質問過程と、

その質問に対する各入札装置からの応答を開札装置で受信する過程と、

開札装置はこれら応答中に入札したという入札装置があるか検証する過程と、

その検証で入札したという入札装置がなければ、 k を - 1 して上記質問過程に戻る過程と、

上記検証で入札したという入札装置があれば、全入札装置に $h^{f(k)}(IV_i)$ の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値 IV_i を用いて $h^{f(k)}(IV_i)$ ($= D_i$) を生成し、この D_i を開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

上記全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する過程と、

これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する過程と、

その検証で全て一致すると、入札したという入札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する過程と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する過程と、

その検証で γ_i と一致すれば、確かに入札装置 j は価格 k で入札したと判断する過程と、

を有することを特徴とする請求項 2 記載の電子競争入札方法。

【請求項 11】 $k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m$, $i \neq j$) に対して、 $E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ を作成する過程と、

これら E_i が共有記録媒体上の入札指標 γ_i と一致するかを検証する過程と、

その検証で γ_i と一致するものが 1 つもなければ、 k を落札価格とし、その k とこの落札価格を提示した入札装置の識別子 ID_i とを出力する過程を有することを特徴とした請求項 10 記載の電子競争入札方法。

【請求項 12】 開札装置に入力された複数の入札指標 γ_i 、識別子 ID_i を共有記録媒体に蓄積する過程と、

パラメータ k を下限値 q にセットする過程と、

全入札装置 i に価格 k で入札したかどうか質問する質問過程と、

その質問に対する各入札装置からの応答を開札装置で受信する過程と、

開札装置はこれら応答中に入札したという入札装置があるかの検証をする過程と、

その検証で入札したという入札装置がなければ、 k を +1 して上記質問過程に戻る過程と、

上記検証で入札したという入札装置があれば、全入札装置に $h^{f(n,k)}(IV_i)$ の提示を要求する。各入札装置は各々の初期値 IV_i を用いて $h^{f(n,k)}(IV_i)$ ($=D_i$) を生成し、この D_i を開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

上記全 D_i に対して $h^{f(n,q-1)-f(n,k)}(D_i)$ を作成する過程と、

これら $h^{f(n,q-1)-f(n,k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する過程と、

その検証で全て一致すると、入札したという入札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する過程と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 γ_j に一致するかど

うか検証する過程と、

その検証で r_i と一致すれば、確かに入札装置 j は価格 k で入札したと判断する過程と

を有することを特徴とする請求項 5 記載の電子競争入札方法。

【請求項 13】 $q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m$, $i \neq j$) に対して、 $E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$ を作成する過程と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する過程と、
その検証で r_i と一致するものが 1 つもなければ、 k を落札価格とし、その k と、この落札価格を提示した入札装置の識別子 ID_i とを出力する過程を有することを特徴とした請求項 12 記載の電子競争入札方法。

【請求項 14】 各入札装置 i は乱数 R_i と入札価格 PR_i とを演算したものを一方向性関数 h 処理して $h(PR_i (+) R_i)$ を求める過程を有し、

上記 $h(PR_i (+) R_i)$ を入札指標 r_i と共に開札装置に入力し、
開札装置に入力された r_i , $h(PR_i (+) R_i)$, ID_i を共有記録媒体に蓄積する過程と、

開札装置は全入力揃うと、全入札装置に PR_i と R_i の提示を要求する過程と、

その提示要求を受けた各入札装置は各々 PR_i と R_i を開札装置に入力する過程と、

開札装置はこれら入力された PR_i , R_i からその最高値 k と、その k を入札した入札装置 (落札装置) j を決定する過程と、

開札装置は全入札装置に $h^{f(k)}(IV_i)$ の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値 IV_i を用いて $h^{f(k)}(IV_i)$ ($=D_i$) を生成して開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

これら全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する過程と、

これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する過程と、

その検証で全て一致すると、落札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する過程と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する過程と、

その検証で一致すれば、確かに入札装置 j は価格 k で入札したと判断する過程と

を有することを特徴とする請求項 2 記載の電子競争入札方法。

【請求項 15】 $k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m$, $i \neq j$) に対して、 $E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ を作成する過程と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する過程と、

その検証で一致するものが 1 つもなければ、 k を落札価格とし、その k と、この落札価格を提示した入札装置の識別子 ID_i を出力する過程を有することを特徴とする請求項 14 記載の電子競争入札方法。

【請求項 16】 各入札装置 i は乱数 R_i と入札価格 PR_i とを演算したものを一方向性関数 h 処理して $h(PR_i (+) R_i)$ を求める過程を有し、

上記 $h(PR_i (+) R_i)$ を入札指標 r_i と共に開札装置に入力し、

開札装置に入力された r_i 、 $h(PR_i (+) R_i)$ 、 ID_i を共有記録媒体に蓄積する過程と、

開札装置は全入力が揃うと、全入札装置に PR_i と R_i の提示を要求する過程と、

その提示要求を受けた各入札装置は各々 PR_i と R_i を開札装置に入力する過程と、

開札装置はこれら入力された PR_i 、 R_i から、その最低値 k と、その k を入札した入札装置（落札装置） j を決定する過程と、

開札装置は全入札装置に $h^{f(n,k)}(IV_i)$ の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値 IV_i を用いて $h^{f(n,k)}(IV_i) (= D_i)$ を生成し、この D_i を開札装置に入力する過程と、

開札装置は入力された全 D_i を共有記録媒体に蓄積する過程と、

上記全 D_i に対して、 $h^{f(n,q-1)-f(n,k)}(D_i)$ を作成する過程と、
これら $h^{f(n,q-1)-f(n,k)}(D_i)$ が共有記録媒体上の C_i と各々一致するか
を検証する過程と、

その検証で全て一致すると、落札装置 j が提示した D_j に対し、 $g(D_j)$ を
生成する過程と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかど
うか検証する過程と、

その検証が一致すれば、確かに入札装置 j は価格 k で入札したと判断する過程
と

を有することを特徴とする請求項 5 記載の電子競争入札方法。

【請求項 17】 $q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m$,
 $i \neq j$) に対して、 $E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$ を作
成する過程と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する過程と、

その検証で一致するものが 1 つもなければ、 k を落札価格として、その k と、
この落札価格を提示した入札装置の識別子 ID_i を出力する過程を有することを
特徴とする請求項 16 記載の電子競争入札方法。

【請求項 18】 入札装置は PR_i と R_i の演算に、入札装置 i が示すこの
入札に関する付加情報 l_i を加え、 $h(PR_i (+) l_i (+) R_i)$ を出力し

開札装置は全入札装置に対し PR_i と R_i のみならず l_i も提示することを要
求することを特徴とする請求項 14 乃至 17 の何れかに記載の電子競争入札方法

【請求項 19】 入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq$
 n なる j に対し、価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、入
札する場合は $b^{(j)}$ を 1 とし、

各入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) は各価格 j を関数 f 処
理して $f(j)$ を求め、各価格 j ごとに価格情報 $b_i^{(j)}$ を生成し、かつ各価格
 j ごとに乱数 $R_i^{(j)}$ を生成し、

各 j ごとに $f(j) (+) b_i^{(j)} (+) R_i^{(j)}$ なる演算を行い、この演算結果を一方向性関数 h で処理して、その処理結果 $h(f(1) (+) b_i^{(1)} (+) R_i^{(1)})$, $h(f(2) (+) b_i^{(2)} (+) R_i^{(2)})$, ..., $h(f(n) (+) b_i^{(n)} (+) R_i^{(n)})$ を上記入札指標とし、

開札装置は各入札装置 i から入力された $\{ID_i, h(f(1) (+) b_i^{(1)} (+) R_i^{(1)}), h(f(2) (+) b_i^{(2)} (+) R_i^{(2)}), \dots, h(f(n) (+) b_i^{(n)} (+) R_i^{(n)})\}$ を共有記録媒体に蓄積する過程と、

パラメータ k を n にセットする過程と、

全入札装置に $R_i^{(k)}$ の提示を要求する提示要求過程と、

その提示要求された各入札装置は各々 $R_i^{(k)}$ を開札装置に入力する過程と、

開札装置はその全 $R_i^{(k)}$ を共有記録媒体に蓄積する過程と、

開札装置は $b_i^{(k)} = 1$ として、各 i に対して入力された $R_i^{(k)}$ を用いて $h(f(k) (+) 1 (+) R_i^{(k)})$ を作成する過程と、

これら $h(f(k) (+) 1 (+) R_i^{(k)})$ が共有記録媒体上に一致するものがあるかどうかを検証する過程と、

その検証で一致するものがなければ k を -1 して上記提示要求過程に戻る過程と、

上記検証で一致するものがあれば、 k を落札価格とし、その k と、その一致したものの $R_i^{(k)}$ を提示した入札装置 i の識別子 ID_i とを出力する過程と

を有することを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 20】 入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq n$ なる j に対し、価格 j を入札しない場合は価格情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、

各入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) は各価格 j を関数 f で処理して $f(j)$ を求め、各価格 j ごとに価格情報 $b_i^{(j)}$ を生成し、かつ各価格 j ごとに乱数 $R_i^{(j)}$ を生成し、

各 j ごとに $f(j) (+) b_i^{(j)} (+) R_i^{(j)}$ なる演算を行い、この演算結果を一方向性関数 h で処理して、その処理結果 $h(f(1) (+) b_i^{(1)} (+) R_i^{(1)})$, $h(f(2) (+) b_i^{(2)} (+) R_i^{(2)})$, ..., $h(f$

n) $(+)$ $b_i^{(n)}$ $(+)$ $R_i^{(n)}$) を上記入札指標とし、

上記乱数 $R_i^{(j)}$ を開札装置に知らせ、

開札装置は各入札装置から入力された

$\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する過程と、

パラメータ k を n にセットする過程と、

全ての i に対して、 $b_i^{(k)} = 1$ として、 $h(f(k)(+)1(+)R_i^{(k)})$ を作成する指標作成過程と、

その $h(f(k)(+)1(+)R_i^{(k)})$ と一致するものが存在するか検証する過程と、

その検証で一致するものがなければ k を -1 して上記指標作成過程に戻る過程と、

上記検証で一致するものがあれば、 $k' \geq k$ である全ての $R_i^{(k')}$ を共有記録媒体に蓄積する過程と、

その一致した時の k を落札価格とし、この k と一致した時の $R_i^{(k)}$ と対応する入札装置の識別子 ID_i とを出力する過程と

を有することを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 2 1】 入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq n$ なる j に対し、価格 j を入札しない場合は価格情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、

各入札装置 i ($i = 1, 2, \dots, m$ 、 m は入札参加数) は各価格 j を関数 f 処理して $f(j)$ を求め、各価格 j ごとに価格情報 $b_i^{(j)}$ を生成し、かつ各価格 j ごとに乱数 $R_i^{(j)}$ を生成し、

各 j ごとに $f(j)(+)b_i^{(j)}(+)R_i^{(j)}$ なる演算を行い、この演算結果を一方向性関数 h で処理して、その処理結果 $h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})$ を上記入札指標とし、

開札装置は各入札装置から入力された

$\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する過程と、

パラメータ k を入札可能な最低価格 1 にセットする過程と、

全入札装置に $R_i^{(k)}$ の提示を要求する提示要求過程と、

その提示要求された各入札装置は各々 $R_i^{(k)}$ を開札装置に入力する過程と、

開札装置はその全 $R_i^{(k)}$ を共有記録媒体に蓄積する過程と、

開札装置は $b_i^{(k)} = 1$ として、各 i に対して入力された $R_i^{(k)}$ を用いて $h(f(k)(+)1(+)R_i^{(k)})$ を作成する過程と、

これら $h(f(k)(+)1(+)R_i^{(k)})$ が共有記録媒体上に一致するものがあるかどうかを検証する過程と、

その検証で一致するものがなければ k を +1 して上記提示要求過程に戻る過程と、

上記検証で一致するものがあれば、 k を落札価格とし、その k と、その一致したものの $R_i^{(k)}$ を提示した入札装置の識別子 ID_i とを出力する過程とを有することを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 22】 入札可能な n 種類の価格を 1, 2, ..., n とし、 $1 \leq j \leq n$ なる j に対し、価格 j を入札しない場合は価格情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、

各入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) は各価格 j を関数 f 処理して $f(j)$ を求め、各価格 j ごとに価格情報 $b_i^{(j)}$ を生成し、かつ各価格 j ごとに乱数 $R_i^{(j)}$ を生成し、

各 j ごとに $f(j)(+)b_i^{(j)}(+)R_i^{(j)}$ なる演算を行い、この演算結果を一方向性関数 h で処理して、その処理結果 $h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})$ を上記入札指標とし、

上記乱数 $R_i^{(j)}$ を開札装置に知らせ、

開札装置は各入札装置から入力された

$\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$

) $b_i^{(2)} (+) R_i^{(2)}$), ..., $h(f(n) (+) b_i^{(n)} (+) R_i^{(n)})$
) } を共有記録媒体に蓄積する過程と、

パラメータ k を入札可能な最低価格 1 にセットする過程と、

全ての i に対して、 $b_i^{(k)} = 1$ として、 $h(f(k) (+) 1 (+) R_i^{(k)})$
)) を作成する指標作成過程と、

その $h(f(k) (+) 1 (+) R_j^{(k)})$ と、共有記録媒体上に一致するものが存在するか検証する過程と、

その検証で一致するものがなければ k を $+1$ して上記指標作成過程に戻る過程と、

上記検証で一致するものがあれば、 $k' \leq k$ である全ての $R_i^{(k')}$ を共有記録媒体に蓄積する過程と、

その一致した時の k を落札価格とし、この k と、一致した時の $R_i^{(k)}$ と対応する入札装置の識別子 ID_i とを出力する過程と、

を有することを特徴とする請求項 1 記載の電子競争入札方法。

【請求項 23】 入札装置 i はその識別子 ID_i を仮識別子登録装置へ送り

仮識別子登録装置は識別子 ID_i に対し、仮識別子 AID_i を発行し、これらの組を記録媒体に保存し、

かつ仮識別子 AID_i を入札装置 i へ送り、

入札装置 i は開札装置に対し、識別子 ID_i として仮識別子 AID_i を入札指標と共に送る

ことを特徴とする請求項 1 乃至 22 の何れかに記載の電子競争入札方法。

【請求項 24】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n とする時、各入札装置 i に対する $C_i = h^{f(n+1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること表わす) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(PRI)}(IV_i))$ ($g(C)$ は C を一方向性関数 g で処理

することを、 PR_i は入札装置 i の入札価格を、 $f(D)$ は D を変数とする関数を表わす) とを共有記録媒体に蓄積する処理と、

処理パラメータ k を上限値 n に設定する処理と、

$\delta_i = g(h^{f(k)}(IV_i))$ を各 IV_i について演算する δ_i 演算処理と、

δ_i が共有記録媒体上の入札指標 r_i と一致するか調べる照合処理と、

上記照合処理で何れの IV_i についても一致するものがなければ上記 k を -1 して上記 δ_i 演算処理に戻る処理と、

上記照合処理で一致すると、その時の k を落札価格とし、その一致した r_i と対応する識別子 ID_i とを出力する処理と、

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 25】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n 、下限値を q とする時、各入札装置 i に対する $C_i = h^{f(n, q-1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること、 $f(C, D)$ は D が大きくなる程 $f(C, D)$ の値が小さな正の整数となる関数を表す) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(n, PR_i)}(IV_i))$ ($g(E)$ は E を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を表わす) とを共有記録媒体に蓄積する処理と、

処理パラメータ k を下限値 q に設定する処理と、

$\delta_i = g(h^{f(n, k)}(IV_i))$ を各 IV_i について演算する δ_i 演算処理と

δ_i が共有記録媒体上の入札指標 r_i と一致するか調べる照合処理と、

上記照合過程で何れの IV_i についても一致するものがなければ上記 k を $+1$ して上記 δ_i 演算処理に戻る処理と、

上記照合処理で一致すると、その時の k を落札価格とし、その一致した r_i と対応する識別子 ID_i とを出力する処理と

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 2 6】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n とする時、各入札装置 i に対する $C_i = h^{f(n+1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること表わす) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(PR_i)}(IV_i))$ ($g(C)$ は C を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を、 $f(D)$ は D を変数とする関数を表わす) とを共有記録媒体に蓄積する処理と、

パラメータ k を上限値 n にセットする処理と、

全入札装置 i に $h^{f(k)}(IV_i)$ の提示を要求する提示要求処理と、

各入札装置 i から入力される $h^{f(k)}(IV_i)$ ($= D_i$) を共有記録媒体に蓄積する処理と、

上記入力された全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する処理と、
これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

その検証で全て一致すると、 $g(D_i)$ を生成する処理と、

その各 $g(D_i)$ が共有記録媒体上の入札指標 r_i に一致するかを検証する処理と、

その検証で一致するものが 1 つもなければ、共有記録媒体上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し、 k を -1 して上記提示要求処理に戻る処理と、

上記検証で一致するものがあればその時の k を落札価格とし、その k と、この落札価格を提示した入札装置の識別子 ID_i とを出力する処理と、

上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 2 7】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n 、下限値を q とする時、各入札装置 i に対する $C_i = h^{f(n,q-1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること、 $f(C, D)$ は D が大きくなる程 $f(C, D)$ の値が小さな正の整数となる関数を表す) を共有記録媒体に蓄積した開札装置のコンピュータが

実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(n, PR_i)}(IV_i))$ ($g(E)$ は E を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を表わす) とを共有記録媒体に蓄積する処理と、

パラメータ k を下限値 q にセットする処理と、

全入札装置 i に $h^{f(n, k)}(IV_i)$ の提示を要求する提示要求処理と、

各入札装置 i より入力された $h^{f(n, k)}(IV_i) (=D_i)$ を共有記録媒体に蓄積する処理と、

上記入力された全 D_i に対して、 $h^{f(n, q-1)-f(n, k)}(D_i)$ を作成する処理と、

これら $h^{f(n, q-1)-f(n, k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

上記検証で全て一致すると、 $g(D_i)$ を生成する処理と、

これら各 $g(D_i)$ が共有記録媒体上の入札指標 r_i に一致するかを検証する処理と、

その検証で一致するものが1つもなければ、共有記録媒体上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し、 k を $+1$ として上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時の k を落札価格とし、その k と、一致した r_i と対応した入札装置の識別子 ID_i とを出力する処理と、

上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 28】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n とする時、各入札装置 i に対する $C_i = h^{f(n+1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること表わす) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(PR_i)}(IV_i))$ ($g(C)$ は C を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を、 $f(D)$ は D を変数とする関数を

表わす) とを共有記録媒体に蓄積する処理と、

パラメータ k を上限値 n にセットする処理と、

全入札装置 i に価格 k で入札したかどうか質問する質問処理と、

その質問に対する入札装置からの応答を入力する処理と、

その入力された応答中に入札したという入札装置があるか検証する処理と、その検証で入札したという入札装置がなければ、 k を -1 して上記質問処理に戻る処理と、

上記検証で入札したという入札装置があれば、全入力装置に $h^{f(k)}(IV_i)$ の提示を要求する処理と、

各入札装置から入力された $h^{f(k)}(IV_i) (=D_i)$ を共有記録媒体に蓄積する処理と、

上記入力された全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する処理と、これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

その検証で全て一致すると、入札したという入札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する処理と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置 j は価格 k で入札したと判断する処理と、

$k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、 $E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ を作成する処理と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する処理と、

その検証で一致するものが1つもなければ、その時の k を落札価格とし、その k と、上記一致した r_i と対応した入札装置の識別子 ID_i とを出力する処理とを上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 29】 入札装置 i ($i = 1, 2, \dots, m, m$ は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n 、下限値を q とする時、各入札装置 i に対する $C_i = h^{f(n,q-1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h 、

で処理すること、 $f(C, D)$ は D が大きくなる程 $f(C, D)$ の値が小さな正の整数となる関数を表す) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(n, PR_i)}(IV_i))$ ($g(E)$ は E を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を表わす) と $h(PR_i (+) R_i)$ (R_i は乱数、 $(+)$ は演算を表わす) とを共有記録媒体に蓄積する処理と、

パラメータ k を下限値 q にセットする処理と、

全入札装置 i に価格 k で入札したかどうか質問する質問処理と、

その質問に対する各入札装置からの応答を入力する処理と、

これら応答中に入札したという入札装置があるかの検証をする処理と、

その検証で入札したという入札装置がなければ、 k を $+1$ して上記質問処理に戻る処理と、

上記検証で入札したという入札装置があれば、全入力装置に $h^{f(n, k)}(IV_i)$ の提示を要求する処理と、

各入札装置からの $h^{f(n, k)}(IV_i) (= D_i)$ を入力する処理と、

その入力された全 D_i を共有記録媒体に蓄積する処理と、

上記入力された全 D_i に対して $h^{f(n, q-1)-f(n, k)}(D_i)$ を作成する処理と

これら $h^{f(n, q-1)-f(n, k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

その検証で全て一致すると、入札したという入札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する処理と、

その $g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置 j は価格 k で入札したと判断する処理と、

$q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、 $E_i = g(h^{f(n, t)-f(n, k)}(h^{f(n, k)}(IV_i)))$ を作成する処理と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する過程と、
その検証で一致するものが1つもなければ、その時の k を落札価格とし、その
 k と、上記一致した r_i と対応した入札装置の識別子 ID_i とを出力する処理と
を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項30】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n とする時、各入札装置 i に対する $C_i = h^{f(n+1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること表わす) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(PR_i)}(IV_i))$ ($g(C)$ は C を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を、 $f(D)$ は D を変数とする関数を表わす) と $h(PR_i (+) R_i)$ (R_i は乱数、 $(+)$ は演算を表わす) とを共有記録媒体に蓄積する処理と、

全入力が揃うと、全入札装置に PR_i と R_i の提示を要求する処理と、

各入札装置 i からの PR_i と R_i を入力する処理と、

これら入力された PR_i 、 R_i からその最高値 k と、 k を入札した入札装置 (落札装置) j を決定する処理と、

全入札装置に $h^{f(k)}(IV_i)$ の提示を要求する処理と、

各入札装置 i からの $h^{f(k)}(IV_i) (= D_i)$ を入力して共有記録媒体に蓄積する処理と、

上記入力した全 D_i に対して、 $h^{f(n+1)-f(k)}(D_i)$ を作成する処理と、

これら $h^{f(n+1)-f(k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

その検証で全て一致すると落札装置 j が提示した D_j に対し、 $g(D_j)$ を生成する処理と、

$g(D_j)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置 j は価格 k で入札したと判断する処理

と、

$k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、
 $E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ を作成する処理と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する処理と、

その検証で一致するものが1つもなければ、その k を落札価格とし、その k との落札価格を提示した入札装置の識別子 ID_i とを出力する処理と

をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項31】 入札装置 i ($i = 1, 2, \dots, m, m$ は入札参加数) に固有の初期値を IV_i 、入札価格の上限値を n 、下限値を q とする時、各入札装置 i に対する $C_i = h^{f(n,q-1)}(IV_i)$ ($h^A(B)$ は B を A 回一方向性関数 h で処理すること、 $f(C, D)$ は D が大きくなる程 $f(C, D)$ の値が小さな正の整数となる関数を表す) を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置 i から入力された、その入札装置 i を特定する識別子 ID_i と、入札指標 $r_i = g(h^{f(n,PR_i)}(IV_i))$ ($g(E)$ は E を一方向性関数 g で処理すること、 PR_i は入札装置 i の入札価格を表わす) と $h(PR_i (+) R_i)$ (R_i は乱数、 $(+)$ は演算を表わす) とを共有記録媒体に蓄積する処理と、

全入力が揃うと、全入札装置に PR_i と R_i の提示を要求する処理と、

各入札装置 i からの PR_i と R_i を入力する処理と、

これら入力された PR_i, R_i からその最低値 k と、 k を入札した入札装置 (落札装置) j を決定する処理と、

全入札装置に $h^{f(n,k)}(IV_i)$ の提示を要求する処理と、

各入札装置 i からの $h^{f(n,k)}(IV_i) (= D_i)$ を入力してその全 D_i を共有記録媒体に蓄積する処理と、

上記入力された全 D_i に対して、 $h^{f(n,q-1)-f(n,k)}(D_i)$ を作成する処理と、

これら $h^{f(n,q-1)-f(n,k)}(D_i)$ が共有記録媒体上の C_i と各々一致するかを検証する処理と、

その検証で全て一致すると落札装置 j が提示した D_j に対し、 $g(D_j)$ を生

成する処理と、

その $g(D_i)$ が共有記録媒体上の入札装置 j の入札指標 r_j に一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置 j は価格 k で入札したと判断する処理と、

$q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、
 $E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(ID_i)))$ を作成する処理と、

これら E_i が共有記録媒体上の入札指標 r_i と一致するかを検証する処理と、

その検証で一致するものが 1 つもなければ、その k を落札価格 k とし、この k とこの落札価格を提示した入札装置の識別子 ID_i とを出力する処理と

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項 3 2】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) を特定する識別子を ID_i とし、入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq n$ なる価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、一方向性関数 h で A を処理することを $h(A)$ とし、 B と C の演算を $B(+)C$ とし、

D を変数とする関数を $f(D)$ とし、 $R_i^{(j)}$ を乱数とし、上記乱数 $R_i^{(j)}$ は開札装置に知らせてあり、

各入札装置 i から入力された

$\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する処理と、

パラメータ k を n に設定する処理と、

全入札装置に $R_i^{(k)}$ の提示を要求する提示要求処理と、

各入札装置 i からの $R_i^{(k)}$ を入力して共有記録媒体に蓄積する処理と、

$b_i^{(k)} = 1$ として、各 i に対して上記入力された $R_i^{(k)}$ を用いて $h(f(k)(+)1(+)R_i^{(k)})$ を作成する処理と、

これら $h(f(k)(+)1(+)R_i^{(k)})$ と一致するものが共有記録媒体上にあるかどうかを検証する処理と、

その検証で一致するものがなければ k を -1 して上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時の k を落札価格とし、その k と、一致した時の $R_i^{(k)}$ と対応した入札装置の識別子 ID_i を出力する処理と
を開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 3 3】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) を特定する識別子を ID_i とし、入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq n$ なる価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、一方向性関数 h で A を処理することを $h(A)$ とし、 B と C の演算を $B(+)C$ とし、

D を変数とする関数を $f(D)$ とし、 $R_i^{(j)}$ を乱数とし、上記乱数 $R_i^{(j)}$ は開札装置に知らせてあり、

各入札装置 i から入力された $\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する処理と、

パラメータ k を n にセットする処理と、

全ての i に対して、 $b_i^{(k)} = 1$ として、 $h(f(k)(+)1(+)R_i^{(k)})$ を作成する指標作成処理と、

その $h(f(k)(+)1(+)R_i^{(k)})$ と一致するものが共有記録媒体上に存在するか検証する処理と、

その検証で一致するものがなければ k を -1 して上記指標作成処理に戻る処理と、

上記検証で一致するものがあれば、 $k' \geq k$ である全ての $R_i^{(k')}$ を共有記録媒体に蓄積する処理と、

その一致した時の k を落札価格とし、その k と、一致した時の $R_i^{(k)}$ と対応する入札装置の識別子 ID_i とを出力する処理と、
を上記開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 3 4】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) を特定する識別子を ID_i とし、入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 1

$\leq j \leq n$ なる価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、一方向性関数 h で A を処理することを $h(A)$ とし、 B と C の演算を $B(+)C$ とし、

D を変数とする関数を $f(D)$ とし、 $R_i^{(j)}$ を乱数とし、

各入札装置 i から入力された $\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する処理と、

パラメータ k を入札可能な最低価格 1 にセットする処理と、

全入札装置に $R_i^{(k)}$ の提示を要求する提示要求処理と、

各入札装置 i からの $R_i^{(k)}$ を入力して共有記録媒体に蓄積する処理と、

$b_i^{(k)} = 1$ として、各 i に対して入力された $R_i^{(k)}$ を用いて $h(f(k)(+)1(+)R_i^{(k)})$ を作成する処理と、

これら $h(f(k)(+)1(+)R_i^{(k)})$ と一致するものが共有記録媒体上にあるかどうかを検証する処理と、

その検証で一致するものがなければ k を + 1 として上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時の k を落札価格とし、その k と、一致したものの $R_i^{(k)}$ と対応した入札装置の識別子 ID_i とを出力する処理とを開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 3 5】 入札装置 i ($i = 1, 2, \dots, m$, m は入札参加数) を特定する識別子を ID_i とし、入札可能な n 種類の価格を $1, 2, \dots, n$ とし、 $1 \leq j \leq n$ なる価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、入札する場合は $b^{(j)}$ を 1 とし、一方向性関数 h で A を処理することを $h(A)$ とし、 B と C の演算を $B(+)C$ とし、

D を変数とする関数を $f(D)$ とし、 $R_i^{(j)}$ を乱数とし、上記乱数 $R_i^{(j)}$ は開札装置に知らせてあり、

各入札装置 i から入力された $\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を共有記録媒体に蓄積する処理と、

パラメータ k を入札可能な最低価格 1 にセットする処理と、
 全ての i に対して、 $b_i^{(k)} = 1$ として $h(f(k) + 1 + R_i^{(k)})$
) を作成する指標作成処理と、
 その $R(f(k) + 1 + R_i^{(k)})$ と一致するものが共有記録媒体上
 に存在するか検証する処理と、
 その検証で一致するものがなければ k を + 1 して上記指標作成処理に戻る処理
 と、
 上記検証で一致するものがあれば、 $k' \leq k$ である全ての $R_i^{(k')}$ を共有記録
 媒体に蓄積する処理と、
 その一致した時の k を落札価格とし、その k と、一致した時の $R_i^{(k)}$ と対応
 する入札装置の識別子 ID_i とを出力する処理と
 を上記開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項 36】 電子競争入札システムの入札装置であって、
 入札価格を生成する入札価格生成装置と、
 上記生成された入札価格を一方向性関数を用いて入札指標に変換する入札価格
 変換装置と、
 上記入札指標と、入札装置を特定する識別子とを開札装置へ送る手段と
 を具備することを特徴とする入札装置。

【請求項 37】 上記入札価格変換装置は、上記入札価格 PR_i を変数とし
 て $f(PR_i)$ を出力する関数 f 処理装置と、
 上記入札装置に固有の初期値 IV_i を、上記 $f(PR_i)$ 回だけ一方向性関数
 h で処理して $h^{f(PR_i)}(IV_i)$ を出力する一方向性関数 h 処理装置と、
 上記一方向性関数 h 処理装置の出力を一方向性関数 g で処理して上記入札指標
 を得る一方向性関数 g 処理装置と
 よりなることを特徴とする請求項 36 記載の入札装置。

【請求項 38】 上記入札価格変換装置は、上記入札価格 PR_i と入札価格
 の上限値 n とを変数として、入力し、 PR_i が大きい程、小さい正の整数値 $f(n, PR_i)$
) を出力する関数 f 処理装置と、
 上記入札装置に固有の初期値 IV_i を、上記 $f(n, PR_i)$ 回だけ一方向性

関数 h で処理して $h^{f(n, PR_i)}(I V_i)$ を出力する一方向性関数 h 処理装置と、

上記一方向性関数 h 処理装置の出力を一方向性関数 g で処理して上記入札指標を得る一方向性関数 g 処理装置と

よりなることを特徴とする請求項 3 6 記載の入札装置。

【請求項 3 9】 乱数 R_i を生成する乱数生成装置と、

上記乱数 R_i と上記入札価格 PR_i とを演算して $PR_i (+) R_i$ を出力する演算装置と、

上記 $PR_i (+) R_i$ を一方向性関数 h で処理して $h(PR_i (+) R_i)$ を出力する一方向性関数 h 処理手段と、

を備え、上記 $h(PR_i (+) R_i)$ をも上記入札指標と共に出力することを特徴とする請求項 3 7 又は 3 8 記載の入札装置。

【請求項 4 0】 上記入札価格変換装置は、

入札可能な n 種類の価格 $1, 2, \dots, n$ の $1 \leq j \leq n$ なる j に対し、価格 j を入札しない場合は価格ビット情報 $b^{(j)}$ を 0 とし、価格 j を入札する場合は $b^{(j)}$ を 1 とし、出力する $b_j^{(j)}$ 生成装置と、

入札装置 i 及び価格 j に固有な乱数 $R_i^{(j)}$ を生成する乱数生成装置と、

価格 j を変数とする関数 $f(j)$ を出力する関数 f 処理装置と、

上記 $f(j)$ と上記 $R_i^{(j)}$ と上記 $b_i^{(j)}$ を入力して演算 $f(j) (+) b_i^{(j)} (+) R_i^{(j)}$ を行う演算装置と、

上記 $f(j) (+) b_i^{(j)} (+) R_i^{(j)}$ を一方向性関数 h で処理して $h(f(j) (+) b_i^{(j)} (+) R_i^{(j)})$ を出力する一方向性関数 h 処理装置と

上記価格 j の $1 \sim n$ のそれぞれについて上記 $h(f(j) (+) b_i^{(j)} (+) R_i^{(j)})$ を求めて、これら n 個を上記入札指標とする制御装置と

よりなることを特徴とする請求項 3 6 記載の入札装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は情報セキュリティ技術を応用して、特にインターネットなどにより

多数の入札者がオンラインでアクセス可能な状況下で、競争入札を実現する方法、その装置及びプログラム記録媒体に関するものである。

【0002】

【従来の技術】

従来の電子競争入札の方法の構成を図1に挙げる。従来の方法では入札公告が各入札装置11₁～11_mに与えられ、各入札装置11₁～11_mはそれぞれその装置の識別子と入札価格とを開札装置12へ送信する。この各データ転送の際に、データを暗号化やデジタル署名が添付され送られていた。開札装置12は各入札装置から受信した入札価格中の最大値（又は最小値）を探し、その値と対応する識別子を出力する。この技術の例として太田と岡本による「電子式入札システム」特開平2-118876号がある。一方、落札価格のみが公となり、これ以外は秘匿可能な技術として以下が挙げられる。

・佐古、「落札値以外を秘匿する全体検証可能な電子入札方式」、暗号と情報セキュリティシンポジウムSCIS'99。

・宮崎、櫻井、「公開揭示版を用いた秘策可能な電子入札システム」、暗号と情報セキュリティシンポジウムSCIS'99。

などに示されている。

【0003】

この発明が対象としている入札方法は次のことを条件としている。

- ・いかなる入札装置も参加可能である。
- ・入札価格を落札の唯一の判断材料とし、これ以外の情報では落札した入札装置は決定されない。
- ・開札装置および仮識別子登録装置は不正を働かず、かつ誤動作を起こさない。
- ・落札した入札装置からの落札価格支払と落札商品の受渡しに関してはこの装置は関与しない。

【0004】

【発明が解決しようとする課題】

入札前に他の入札装置の情報を得、有利に入札を行うことを防止（公平性）。

落札価格と決定に関する不正防止（正当性）。

開札時にその価格で入札したことを認めない行為防止（否認不可性）。

各入札装置の識別子情報漏洩防止（匿名性）。

【0 0 0 5】

同一入札装置による複数回の入札防止。

【0 0 0 6】

【課題を解決するための手段】

この発明によれば入札装置において、入札価格と、一方向性関数を利用して入札指標に変換し、開札装置では、その入札指標を利用して、非落札価格を全入札装置に知らせることなく落札価格を決める。

【0 0 0 7】

【発明の実施の形態】

実施例 1

電子競争入札装置は図 1 に示した場合と同様に m 個の入札装置 $11_1 \sim 11_m$ と開札装置 12 とから成り、これら間に相互に通信可能とする。

この装置は、図 2 に示す流れに従って動作する。

【0 0 0 8】

Step 1 : 各入札装置 $11_1 \sim 11_m$ に入札公告を入力する。

Step 2 : 各入札装置 11_i ($i = 1, 2, \dots, m$) は入力である入札の内容を記述された入札公告に対して、入札価格を生成し、入札価格と自分を特定できる識別子を開札装置 12 に送信する。

Step 3 : 開札装置 12 は入力である複数の入札価格と各々に対応した識別子に対して、全入札価格中の最大値（または最小値）を求めて落札価格を決める。

【0 0 0 9】

Step 4 : その落札価格とこれを提示した入札装置の識別子を出力する。

入札指標

以上の処理は従来技術と同様である。このような処理では各入札装置は他の入札装置の入札価格を知ることができる。そこでこの発明では入札価格を入札指標に変換して用いる。

【0010】

図3に示すように、入札装置11_i 内において入札価格生成装置13より生成された入札価格は入札価格変換装置14に入力され、一方向性関数を用いて整数の入札指標に変換して出力し、この入札指標と識別子を開札装置12へ送る。開札装置12は全入札指標から落札価格を決める。

入札価格変換装置14は図4に示すように入札価格生成装置13から初期値 IV_i と、入札価格 PR_i が入力され、 IV_i を初期値として、これに対し、 PR_i に応じた関数だけ一方向性関数演算がなされる。一方向性関数は x が与えられたとき、 x から $y (=h(x))$ を求めることは容易であるが、逆に y が与えられた時に、 $y = h(x)$ となる x を求めるのは計算量が極めて大きなものである。また $h(\dots h(h(h(IV_i))) \dots)$ のように初期値 IV_i を関数 h で k 回処理した出力値を $h^k(IV_i)$ と表わす。

【0011】

入札価格変換装置14の具体例を図5に、その処理手順を示す。

Step 1: 入札価格 PR_i と初期値 IV_i を入力する。

Step 2: 関数 f 処理装置15で PR_i に対し、関数演算 $f(PR_i)$ を行う。 $f(PR_i)$ は例えば入札価格が100円、200円、300円…の場合に $PR_i / 100$ の演算を行い、 $f(PR_i)$ は1, 2, 3, …となり処理が簡単になる。

【0012】

Step 3: 一方向性関数 h 処理装置16において、変数 t を0とし、初期値 IV_i を r_i とし、以下のStep 4とStep 5を繰返す。

Step 4: t が $f(PR_i)$ 以下であるかを判定し、

Step 5: $t \leq f(PR_i)$ であればその時の $h(r_i)$ を r_i とし、また t を+1してステップS4に戻る。

【0013】

Step 6: $t \leq f(PR_i)$ でなくなると、その時は $r_i = h^{f(PR_i)}(IV_i)$ であり、これを一方向性関数 g 処理装置17で処理し $r_i = g(r_i)$ とする。

Step 7: その r_i を入札指標として出力する。

開札装置 (最高値落札)

図 7 に開札装置 1 2 の構成を示す。その装置 1 2 は制御装置 2 1 と、この制御装置 2 1 にそれぞれ接続された一方向性関数 h 処理装置 2 2、一方向性関数 g 処理装置 2 3、減算器 2 4、記録媒体 2 5、関数 f 処理装置 2 6 と、メモリ手段 3 5 とから成る、関数 f 処理装置 2 6、一方向性関数 h 処理装置 2 2、一方向性関数 g 処理装置 2 3 は順次直列に接続されている。また記録媒体 2 5 以外の部分は落札価格選択装置 2 7 を構成する。各入札装置 1 1 _{i} の初期値 IV_i は予め何らかの手段により開札装置 1 2 の記録媒体 2 5 に記録されている。

【0014】

この装置の動作の手順を図 8 に示す。この例は最高の入札価格を落札価格とする場合である。

Step 1: 制御装置 2 1 は外部から入力された入札指標 r_i , 識別子 ID_i を他の装置から参照可能な共有の記録媒体 2 5 に記録する。

Step 2: 制御装置 2 1 は記録媒体 2 5 から入札価格の上限値 n をメモリ手段 3 5 から読み出し、 k に n を代入する。

【0015】

Step 3: 制御装置 2 1 は $k > 0$ かを判定し、

Step 4: $k > 0$ であれば、 i を 1 とし、

Step 5: $i > m$ かを判定し、

Step 6: $i > m$ でなければ t を 0 とし、 IV_i を記録媒体 2 5 から読出して $\delta_i = IV_i$ とする。

【0016】

Step 7: 制御装置 2 1 は関数 f 処理装置 2 6 に k を入力して $f(k)$ を求める。

Step 8: 制御装置 2 1 は一方向性関数 h 処理装置 2 2 に δ_i と $f(k)$ を入力して、 δ_i を初期値として、これを $f(k)$ 回、一方向性関数 h で処理して $\delta_i = h^{f(k)}(IV_i)$ を求める。

【0017】

Step 9: 一方向性関数 h 処理装置 22 の出力 $\delta_i = h^{f(k)}(IV_i)$ を一方向性関数 g 処理装置 23 に入力して、一方向性関数 g で処理して $\delta_i = g(h^{f(k)}(IV_i))$ を出力する。

Step 10: 制御装置 21 は $\delta_i = g(h^{f(k)}(IV_i))$ と同じ値が記録媒体 25 上の r_i 中に存在するかの照合を行う。

【0018】

Step 11: 記録媒体 25 上に δ_i と同一の r_i が存在しなければ i を +1 してスナップ S5 に戻り次の IV_i について同様のことを行う。

Step 12: ステップ S5 で i が m より大になると制御装置 21 は k を減算器 24 に入力して、 k から 1 を減算して ($k \leftarrow k - 1$) として、ステップ S3 に進み、減算された k について、 $\delta_i = g(h^{f(k)}(IV_i))$ と同一の r_i が記録媒体 25 にあるかの検査を同様にを行う。

【0019】

Step 13: ステップ S10 で δ_i と同じ値の r_i が記録媒体 25 上に存在すれば、制御装置 21 はこれを落札価格と見なし、この時の k と、合致した r_i に対応する ID_i とを出力して終了する。

なおステップ S3 で $k > 0$ でなくなれば、その時の入札価格 IV_i は全て上限値 n 以上であったことになり、その競争入札は落札がなかったことになる。

【0020】

以上のようにして、上限値 n の入札価格 IR_i があるかをまず調べ、なければ n から単位値 1 を減算した値の入札価格 IR_i があるか調べ、なければ、更に単位値 1 を減算した値について調べると、順次低い値で入札価格 IR_i があるかを調べて行くことにより、最高の入札価格 IR_i を探することができる。

また、各入札装置 11_i が $h^{f(n+1)}(IV_i)$ を予め公開しておき、開札装置 12 が落札価格 k 、 ID_i の他に $h^{f(k)}(IV_i)$ も公開すると、その $h^{f(k)}(IV_i)$ に対し、 $f(n+1) - f(k)$ 回一方向性関数 h の処理を行ってその値 $h^{f(n+1)-f(k)}h^{f(k)}(IV_i)$ が公開されている $h^{f(n+1)}(IV_i)$ と一致すれば、その開札処理が正しく行われたことを納得することができる。

【0021】

次に最低の入札価格を落札価格とする場合に用いる入札指標を生成する入札価格変換装置 1 4 の例を図 9 に示す。この場合も関数 f 処理装置 3 1 と、一方向性関数 h 処理装置 1 6 と、一方向性関数 g 処理装置とを備え、更にメモリ手段 3 2 を備えている。メモリ手段 3 2 には入札価格の上限値 n が格納され、関数 f 処理装置 3 1 には入札価格 PR_i の他に上限値 n も入力される。関数 f 処理装置 3 1 は PR_i と n を変数とする関数 $f(n, PR_i)$ を生成する。関数 $f(n, PR_i)$ は、 $(n - PR_i)$ や n / PR_i などのように PR_i が大きい程、小さな正の整数値となるような関数である。

【0022】

この装置は図 6 に示した動作と同様な動作を行う。ただステップ S 2 で入札価格 PR_i と、メモリ手段 3 2 から読み出した n とから $f(n, \alpha_i)$ を生成し、以下、図 6 中の $f(PR_i)$ の代りに $f(n, PR_i)$ が用いられる。従って一方向性関数 h 処理装置 1 6 は $h^{f(n, PR_i)}(IV_i)$ を出力し、一方向性関数 g 処理装置 1 7 は $g(h^{f(n, PR_i)}(IV_i))$ を出力する。

【0023】

開札装置（最低値落札）

次に図 9 に示した入札価格変換装置により生成された入札指標を入力とし、最低入札価格を落札価格とする開札装置 1 2 を図 1 0 に示す。図 9 において図 7 と対応する部分に同一番号を付けてある。関数 f 処理装置 2 6 の代りに、 n と k を入力し、 $f(n, k)$ を生成する関数 f 処理装置 3 3 が用いられ、また減算器 2 4 の代りに k を $+1$ する加算器 3 4 が用いられている点が異なる。

【0024】

この装置は図 1 1 に示すように実行される。入札指標 $\gamma_i = g(h^{f(n, IR_i)}(IV_i))$ における $f(n, IR_i)$ はこの例では $n - IR_i$ とする。

Step 1: 制御装置 2 1 は外部から入力された各入札指標 γ_i , と対応識別子 ID_i を記録媒体 2 5 に記録する。

Step 2: 制御装置 2 1 は記録媒体 2 5 から落札上限値 n と落札下限値 q をメモリ手段 3 5 から読み出し、 k に q を代入する。

Step 3: 制御装置 2 1 は $n > k$ かを判定し、

Step 4: $n > k$ であれば i を 1 とし、

Step 5: $i > m$ かを判定し、

Step 6: $i > m$ でなければ t を 0 とし、 IV_i を記録媒体 25 から読出して $\delta_i = IV_i$ とする。

Step 7: 制御装置 21 は関数 f 処理装置 33 に n, k を入力して $f(n, k)$ を求める。この例では $f(n, k) = n - k$ である。

Step 8: 制御装置 21 は一方向性関数 h 処理装置 22 に δ_i と $f(n, k)$ を入力して、 δ_i を初期値として、これを $f(n, k)$ 回、一方向性関数 h で処理して $\delta_i = h^{f(n,k)}(IV_i)$ を求める。

Step 9: 一方向性関数 h 処理装置 22 の出力 $\delta_i = h^{f(n,k)}(IV_i)$ を、一方向性関数 g 処理装置 23 に入力して、一方向性関数 g で処理して $\delta_i = g(h^{f(n,k)}(IV_i))$ を出力する。

Step 10: 制御装置 21 は $\delta_i = g(h^{f(n,k)}(IV_i))$ と同じ値が記録媒体 25 上の r_i 中に存在するかの照合を行う。

Step 11: 記録媒体 25 上に δ_i と同一の r_i が存在しなければ i を +1 してステップ S5 に戻り、次の IV_i について同様のことを行う。

Step 12: ステップ S5 で $i > m$ となると制御装置 21 は k を加算器 34 に入力して k を +1 して ($k \leftarrow k + 1$) として、ステップ S3 に戻り、加算された k について $\delta_i = g(h^{f(n,k)}(IV_i))$ と同一の r_i が記録媒体 25 上にあるかの検査を同様に行う。

Step 13: ステップ S10 で δ_i と同じ値の r_i が記録媒体上に存在すれば、制御装置 21 はこれを落札価格と見なし、この時の k と、合致した r_i に対応する ID_i とを出力して終了する。

【0025】

なおステップ S3 で $n > k$ でなくなれば、その時の入札価格 IV_i は全て下限値 q 以下か、上限値 n 以上であったことになり、その競争入札は落札がなかったことになる。

以上のようにしてまず k を下限値 q とし、 q と同一の入札価格 PR_i があるかを調べ、なければ k を単位値 1 だけ大として入札価格 PR_i があるかを調べるこ

とを順次行うことにより、最低の入札価格、つまり落札価格をもとめることができる。

【0026】

このように $h^{f(n,k)}(IV_i)$ とし、 $k=q$ (下限値) から調べるが、一方向性関数 h の処理回数 $f(n, k)$ は大きな値から、対応する入札指標 r_i があるかを調べているため、他の入札装置の入札価格が知られることがない。つまり $h^{f(k)}(IV_i)$ とし、 $k=q$ から調べて、最低価格と対応する r_i を探す場合は、一方向性関数は処理回数が少ない値から回数が多い値は容易に求めることができるため、他の入札装置の入札価格を求めることができるおそれがある。

実施例 2

上述では開札装置 12 は各入札装置 11_i の初期値 IV_i を知っている必要があった。実施例 2 では開札装置 12 は初期値 IV_i を知る必要がない。

【0027】

最高価格を落札価格とする場合についてまず述べる。

開札装置 12 は図 12 に示すように、制御装置 21、一方向性関数 h 処理装置 22、一方向性関数 g 処理装置 23、減算器 24、メモリ手段 35、および他の装置からも参照可能な共有記録媒体 25 から構成されている。

この開札装置 12 は図 13 に示すように動作する。

【0028】

まず開札装置に入力された複数の入札データ (入札指標 $r_i = g(h^{f(Pri)}(IV_i))$ 、識別子 ID_i) が共有記録媒体 25 に蓄積される (S1)。また全入札装置と共有されている $h^{f(n+1)}(IV_i)$ は予め C_i として共有記録媒体 25 に蓄積されている。ここでは m 個の入札があったとし、 $i=1, 2, \dots, m$ とする。カウンタの計数値 k を上限値 n にセットする (S2)。

【0029】

全入札装置 11_i に $h^{f(k)}(IV_i)$ の提示を要求する (S3)。各入札装置 11_i は各々の初期値 IV_i を用いて $h^{f(k)}(IV_i) (=D_i)$ を生成し、この D_i を開札装置 12 に入力する。

開札装置 12 は入力された全 D_i を共有記録媒体 25 に蓄積する (S4)。ま

た全 D_i に対して、一方向性関数 h 処理装置 22 を用いて、 $h^{f(n+1)-f(k)}(D_i)$ を作成し (S5)、この $h^{f(n+1)-f(n)}(D_i)$ が共有記録媒体 25 上の C_i と各々一致するかを検証し (S6)、全て一致したならば、全ての D_i は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【0030】

ステップ S6 で全てが一致すれば一方向性関数 g 処理装置 23 を用いて、 $g(D_i)$ を生成し (S7)、その各 $g(D_i)$ が共有記録媒体 25 上の入札データ中の入札指標 r_i に一致するかを検証する (S8)、一致するものが 1 つもなければ、共有記録媒体 25 上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し (S9)、減算器 24 により $k \leftarrow k - 1$ としてステップ S3 に戻る (S10)。ステップ S8 で一致するものがあればその時の k を落札価格とし、その k と、この落札価格を提示した入札装置 11_i の識別子 ID_i を出力する (S11)。

【0031】

この場合は開札装置 12 にも落札価格以外の入札価格が知られないことになる。

次にこの例において、最低価格を落札価格とする場合を述べる。図 14 に開札装置の構成を示す。図 12 との相違は減算器 24 の代りに加算器 34 が設けられている点である。

【0032】

この開札装置 12 は図 15 に示すように動作する。まず開札装置に入力された複数の入札データ (入札指標 $r_i = g(h^{f(n, Pri)}(IV_i))$ 、識別子 ID_i) が共有記録媒体 25 に蓄積される (S1)。また全入札装置と共有されている $h^{f(n, q-1)}(IV_i)$ は予め C_i として共有記録媒体 25 に蓄積されている。ここでは m 個の入札があったとし、 $i = 1, 2, \dots, m$ とする。カウンタ k に下限値 q をセットする (S2)。

【0033】

全入札装置 11_i に $h^{f(n, k)}(IV_i)$ の提示を要求する (S3)。各入札装置 11_i は各々の初期値 IV_i を用いて $h^{f(n, k)}(IV_i)$ ($= D_i$) を生成し、この D_i を開札装置 12 に入力する。

開札装置 1 2 は入力された全 D_i を共有記録媒体 2 5 に蓄積する (S 1 5)。
また全 D_i に対して、一方向性関数 h 処理装置 2 2 を用いて、 $h^{f(n,q-1)-f(n,k)}$
) (D_i) を作成し (S 5)、これが共有記録媒体 2 5 上の C_i と各々一致する
かを検証する (S 6)。その検証で全て一致したならば、全ての D_i は正しいと
し、以下を続行する。なお、正しくなければエラーを返して終了する。

【0 0 3 4】

ステップ S 6 で全て一致したならば一方向性関数 g 処理装置 2 3 を用いて、 g
(D_i) を生成し (S 7)、各 $g(D_i)$ が共有記録媒体 2 5 上の入札データ中
の入札指標 r_i に一致するかを検証する。一致するものが 1 つもなければ、共有
記録媒体 2 5 上の C_i を D_i で上書き ($C_i \leftarrow D_i$) し (S 9)、加算器 1 4 に
より $k \leftarrow k + 1$ としてステップ S 3 に戻る (S 1 0)。ステップ S 8 で一致する
ものがあればその時の k を落札価格とし、その k と、この落札価格を提示した入
札装置の識別子 ID_i を出力する (S 1 1)。

実施例 3

この実施例 3 では開札装置 1 2 は初期値 IV_i を知る必要がなく、落札価格以
外の入札価格が知られず、しかも通信を簡単にする。

【0 0 3 5】

まず最大値を落札価格とする場合について述べる。

開札装置 1 2 は図 1 6 に示すように図 1 2 に対し、関数 f 処理装置 2 6 が設け
られている点が異なる。

この装置の動作は図 1 7 に示すように、まず開札装置に入力された複数の入札
データ (入札指標 $r_i = g(h^{f(PRI)}(IV_i))$ 、識別子 ID_i) が共有記録
媒体 2 5 に蓄積される (S 1)。また全入札装置 1 1_i と共有されている $h^{f(n+1)}$
) (IV_i) は予め C_i として共有記録媒体 2 5 に蓄積されている。ここでは m
個の入札があったとし、 $i = 1, 2, \dots, m$ とする。カウンタの計数值 k を上限
値 n にセットする (S 2)。

【0 0 3 6】

全入札装置 1 1_i に価格 k で入札したかどうか尋ねる (S 3)。価格 k で入札
したという入札装置が 1 つもなければ (S 4)、減算器 2 4 により $k \leftarrow k - 1$ と

してステップ S3に戻る (S5)。

ステップ S4で価格 k で入札したという入札装置があれば、全入札装置 11_i に $h^{f(k)}(IV_i)$ の提示を要求する (S6)。各入札装置 11_i は各々の初期値 IV_i を用いて $h^{f(k)}(IV_i) (=D_i)$ を生成し、この D_i を開札装置 12に入力する。

【0037】

開札装置 12は入力された全 D_i を共有記録媒体 25に蓄積する (S7)。また全 D_i に対して、一方向性関数 h 処理装置 22を用いて、 $h^{f(n+1)-f(k)}(D_i)$ を作成し (S8)、これが共有記録媒体 25上の C_i と各々一致するかを検証し (S9)、全て一致したならば、全ての D_i は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【0038】

ステップ S9で全て一定ならばまず、入札したという入札装置 11_j が提示した D_j に対し、一方向性関数 g 処理装置 23を用いて、 $g(D_j)$ を生成し (S10)、 $g(D_j)$ が共有記録媒体 25上の入札装置 11_j の入札データ中の入札指標 r_j に一致するかどうかを検証する (S11)。一致すれば、確かに入札装置 11_j は価格 k で入札したと判断する。一致しなければエラーを返して終了する。

【0039】

必要に応じて、次に他の (11_j 以外の) 入札装置 11_i が、価格 k 以上で入札していなかったかどうかを、次のように検証する。

$k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、 $g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ が共有記録媒体 25上の入札指標 r_i と一致するかを検証し (S12)、一致するものがあれば、エラーを返して終了する。一致するものが1つもなければ、落札価格 k と、この落札価格を提示した入札装置の識別子 ID_i を出力する (S13)。

【0040】

この検証を行えば、例えば k で入札したかの問い合わせに対して入札したとの応答をしそこなった場合が救済される。この検証を行わない場合はステップ S11

で k で入札したと判断した時に k と ID_i を出力する。

このようにして開札装置 1 2 にも落札価格以外の入札価格が知れずに、かつ通信量を削減することができる。

【0 0 4 1】

次にこの実施例 3 において最低価格を落札価格とする場合を説明する。

開札装置 1 2 は図 1 8 に示すように図 1 6 に対し、減算器 2 4 の代りに加算器 3 4 が用いられる点が相違する。この装置の動作を図 1 9 に示す。まず開札装置 1 2 に入力された複数の入札データ（入札指標 $r_i = g(h^{f(n, PR_i)}(IV_i))$ ）、識別子 ID_i ）が共有記録媒体 2 5 に蓄積される（S 1）。また全入札装置と共有されている $h^{f(n, q-1)}(IV_i)$ は予め C_i として記録媒体 2 5 に蓄積されている。ここでは m 個の入札があったとし、 $i = 1, 2, \dots, m$ とする。カウンタの計数値 k に下限値 q をセットする（S 2）。

【0 0 4 2】

全入札装置 1 1_i に価格 k で入札したかどうか尋ねる（S 3）。価格 k で入札したという入札装置が 1 つもなければ（S 4）、加算器 3 4 により $k \leftarrow k + 1$ とし、ステップ S 3 に戻る（S 5）。

価格 k で入札したという入札装置があれば、全入札装置 $h^{f(n, k)}(IV_i)$ の提示を要求する（S 6）。各入札装置 1 1_i は各々の初期値 IV_i を用いて $h^{f(n, k)}(IV_i)$ （ $= D_i$ ）を生成し、この D_i を開札装置 1 2 に入力する。

【0 0 4 3】

開札装置 1 2 は入力された全 D_i を共有記録媒体 2 5 に蓄積する（S 7）。また全 D_i に対して、一方向性関数 h 処理装置 2 2 を用いて、 $h^{f(n, q-1)-f(n, k)}(D_i)$ を作成し（S 8）、これが共有記録媒体 2 5 上の C_i と各々一致するかを検証し（S 9）、全て一致したならば、全ての D_i は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【0 0 4 4】

ステップ S 9 で全て一致すれば、入札したという入札装置 1 1_j が提示した D_j に対し、一方向性関数 g 処理装置 2 3 を用いて、 $g(D_j)$ を生成し（S 1 0）、 $g(D_j)$ が共有記録媒体 2 5 上の入札装置 1 1_j の入札データ中の入札指

標 r_j に一致するかどうかを検証する (S 1 1)。一致すれば、確かに入札装置 1 1 j は価格 k で入札したと判断する。一致しなければエラーを返して終了する。

【0 0 4 5】

必要に応じて次に他の (1 1 j 以外の) 入札装置 1 1 i が、価格 k 以下で入札していなかったかどうかを、次のように検証する。

$q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m$, $i \neq j$) に対して、 $g(h^{f(n,t)-f(n,h)}(h^{f(n,k)}(IV_i)))$ が共有記録媒体 2 5 上の入札指標 r_i と一致するかを検証し、一致するものがあれば、エラーを返して終了する。一致するものが 1 つもなければ、落札価格 k と、この落札価格を提示した入札装置 1 1 i の識別子 ID_i を出力する (S 1 3)。

【0 0 4 6】

落札装置にも落札価格以外の入札価格が知れずに、かつ通信量を削減し、最低入札価格を落札価格として求めることができる。

実施例 4

この実施例 4 は開札装置 1 2 における処理を簡単にし、かつ通信量を削減することを可能としたものである。

【0 0 4 7】

図 2 0 に示すように各入札装置 1 1 i はその入札装置 1 1 i のみが知る乱数 R_i を乱数生成装置 1 8 で生成し、その R_i と入札価格 PR_i を用い演算装置 1 9 でビット連結、加算、乗算などの適当な演算 (これを (+) で表わす) を行い、その結果に対し、一方向性関数 h 処理を行い、その結果 $h(PR_i (+) R_i)$ を入札指標 $r_i = g(h^{f(PR_i)}(IV_i))$ と識別子 ID_i と共に開札装置 1 2 へ送る。

【0 0 4 8】

この場合の開札装置 1 2 の機能構成を図 2 1 に示し、その動作の流れを図 2 2 に示す。各入札装置 1 1 i ごとに、 $r_i = g(h^{f(PR_i)}(IV_i))$ 、 $h(PR_i (+) R_i)$ 、 ID_i を入力として受け付け、共有記録媒体 2 5 に蓄積する (S 1)。また全入札装置 1 1 i と共有されている $h^{f(n+1)}(IV_i)$ は予め C_i

として共有記録媒体 25 に蓄積されている。

【0049】

全入力揃うと、全入札装置 11_i に入札価格 PR_i と乱数 R_i の提示を要求する (S2)。各入札装置 11_i は各々 PR_i と R_i を開札装置 12 に入力し (S3)、この時点で開札装置 12 には全入札価格が分かり、開札装置 12 は最高値を k とおき、 k を入札した入札装置 (落札装置) を 11_j とする (S4)。なおこの PR_i の提示前は各入札装置は他の入札装置の入札価格を知ることはいない。

【0050】

開札装置 12 は全入札装置 11_i に $h^{f(k)}(IV_i)$ の提示を要求する (S5)。各入札装置 11_i は各々の初期値 IV_i を用いて $h^{f(k)}(IV_i)$ ($=D_i$) を生成し、この D_i を開札装置 12 に入力し、開札装置 12 は入力された全 D_i を共有記録媒体 25 に蓄積する (S6)。また全 D_i に対して、一方向性関数 h 処理装置 22 を用いて、 $h^{f(n+1)-f(k)}(D_i)$ を作成し (S7)、これが共有記録媒体 25 上の C_i と各々一致するかを検証 (S8)。全て一致したならば、全ての D_i は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。なお、関数 f 処理装置 26 に $n+1$ と k を入力して $f(k)$ 、 $f(n+1)$ を生成し、減算器 37 で $f(n+1) - f(k)$ を作って一方向性関数 h 処理装置 22 へ入力する。

【0051】

ステップ S8 で全てが一致すれば、まず、落札装置 11_j が提示した D_j に対し、一方向性関数 g 処理装置 23 を用いて、 $g(D_j)$ を生成し (S9)、 $g(D_j)$ が共有記録媒体 25 上の 11_j の入札データ中の入札指標 r_j に一致するかどうか検証する (S10)。一致すれば、確かに入札装置 11_j は価格 k で入札したと判断する。一致しなければエラーを返して終了する。

【0052】

必要に応じて次に他の (11_j 以外の) 入札装置 11_i が、価格 k 以上で入札していなかったかどうかを、次のように検証する。

$k \leq t \leq n$ である t と、 j を除く全ての i ($1 \leq i \leq m$, $i \neq j$) に対して、

$g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ が共有記録媒体 2 5 上の入札指標 r_i と一致するかを検証し (S 1 1)、一致するものがあれば、エラーを返して終了する。一致するものが 1 つもなければ、落札価格 k と、この落札価格を提示した入札装置 1 1_i の識別子 ID_i を出力する (S 1 2)。なお $g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ の演算は制御装置 2 1''、関数 f 処理装置 2 6'、一方向性関数 h 処理装置 2 2'、一方向性関数 g 処理装置 2 3で行う。

【0 0 5 3】

仮りに i が $h(PR' (+) R_i)$ と $r_i = g(h^{f(PR_i)}(IV_i))(PR_i' > PR_i)$ を出力し、 PR_i と R_i の提示要求に対し、 PR' を提示し、これが最高値となった場合に、 $h^{f(k)}(IV_i)$ の提示要求に対し、 $h^{f(PR_i)}(IV_i)$ を提示すると、 PR_i' より低い PR_i で落札してしまうおそれがあるが、ステップ S 1 1 の検証によりこのような悪為は防止できる。

【0 0 5 4】

開札装置 1 2 は、落札価格およびこれを提示した入札装置を PR_i と R_i から簡単に特定でき、かつ通信量を削減することができ、 PR_i 、 R_i から決定した落札価格と入札装置が真のものであるかを検証することができる。

次にこの実施例 4 で最低入札価格を落札価格とする場合の開札装置 1 2 における処理手順を図 2 3 を参照して説明する。この場合各入札装置 1 1_i ごとに、 $r_i = g(h^{f(n, PR_i)}(IV_i))$ と $h(PR_i (+) R_i)$ と ID_i を入力として受け付け、記録媒体 2 5 に記録する (S 1)、また全入札装置 1 1_i と共有されている $h^{f(n, q-1)}(IV_i)$ は予め C_i として共有記録媒体 2 5 に蓄積されている。

【0 0 5 5】

全入力が揃うと、全入札装置 1 1_i に入札価格 PR_i と乱数 R_i の提示を要求する (S 2)。各入札装置 1 1_i は各々 PR_i と R_i を開札装置 1 2 に入力し (S 3)、この時点で開札装置 1 2 には全入札価格 PR_i が分かり、開札装置 1 2 はその最低値を k とおき、 k を入札した入札装置 (落札装置) を 1 1_j とする (S 4)。

【0 0 5 6】

開札装置 12 は全入札装置 11_i に $h^{f(n,k)}(IV_i)$ の提示を要求する (S5)。各入札装置 11_i は各々の初期値 IV_i を用いて $h^{f(n,k)}(IV_i)$ ($=D_i$) を生成し、この D_i を開札装置 12 に入力。開札装置 12 は入力された全 D_i を共有記録媒体 25 に蓄積する (S6)。また全 D_i に対して、一方向性関数 h 処理装置を用いて、 $h^{f(n,q-1)-(n,k)}(D_i)$ を作成し (S7)、これが共有記録媒体 25 上の C_i と各々一致するかを検証し (S8)、全て一致したならば、全ての D_i は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【0057】

ステップ S8 で全て一致するならばまず、落札装置 11_j が提示した D_j に対し、一方向性関数 g 処理装置を用いて、 $g(D_j)$ を生成し (S9)、 $g(D_j)$ が共有記録媒体上の落札装置 11_j の入札データ中の入札指標 r_j に一致するかどうか検証する (S10)。一致すれば、確かに 11_j は価格 k で入札したと判断する。一致しなければエラーを返して終了する。

【0058】

必要に応じて次に他の (11_j 以外の) 入札装置 11_i が、価格 k 以下で入札していなかったかどうかを、次のように検証する。

$q \leq t \leq k$ である t と、 j を除く全ての i ($1 \leq i \leq m, i \neq j$) に対して、 $g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$ が共有記録媒体 25 上の入札指標 r_i と一致するかを検証し (S11)、一致するものがあれば、エラーを返して終了する。一致するものが 1 つもなければ、落札価格 k と、この落札価格を提示した入札装置 11_i の識別子 ID_i を出力する (S12)。

【0059】

この最低入札価格を落札価格とし、それが真であることを検証することができる。

実施例 4 において各入札装置 11_i から $h(PR_i(+)R_i)$ も出力するようにしたが、 $h(PR_i(+)R_i)$ の代りに $h(PR_i(+)1_i(+)R_i)$ を出力するようにしてもよい。ただし、 1_i は入札者 i が示すこの入札に関する付加情報であり、納品可能商品個数などである。この場合の開札処理は図 22

、図 23 に示した場合とほぼ同様であるが、全ての入札装置から入札データ r_i 、 ID_i 、 $h(PR_i (+) l_i (+) R_i)$ を受け取った後に、全入札装置 11_i に対し、 PR_i 、 l_i 、 R_i の提示を要求する点が異なるだけである。

実施例 5

この実施例 5 は入札可能な n 種類の価格について全てを含む入札指標を送出する。図 24 に示すように入札装置 11_i の入札価格変換装置 14 は、制御装置 41、乱数生成装置 42、一方向性関数 h 処理装置 43、関数 f 処理装置 44、 $b_i^{(j)}$ 、生成装置 45、 $(+)$ 演算装置 46、加算器 47 から成る。関数 f 処理装置 41 は図 5 中の関数 f 処理装置 15 と同様のものである。

【0060】

入札可能な n 種類の価格 $1, 2, \dots, n$ のうち、入札装置 11_i が実際に入札しようとしている価格を PR_i とする。また、入札装置 11_i において、 $1 \leq j \leq n$ なる j に対して、価格 j を入札しない場合は $b^{(i)} = 0$ 、価格 j を入札する場合は $b^{(j)} = 1$ と $b^{(j)}$ を定義する。従って $1 \leq j \leq n$ なる j に対して、 $b^{(j)}$ は唯 1 つのみ 1 である。 $R_i^{(j)}$ を入札装置 11_i しか知らず j ごとに異なる乱数として、全ての入札可能価格に対し、入札装置 11_i は $\{ID_i, h(f(1)(+) b_i^{(1)} (+) R_i^{(1)}), h(f(2)(+) b_i^{(2)} (+) R_i^{(2)}), \dots, h(f(n)(+) b_i^{(n)} (+) R_i^{(n)})\}$ を出力する。

【0061】

図 25 を参照して、この n 個からなる入札指標の生成手順を説明する。入札価格 PR_i が決定入力され (S1)、価格パラメータ j を 1 とし (S2)、 $j \leq n$ か否かを調べ (S3)、 $j \leq n$ であれば、関数 f 処理装置 44 に j を入力して $f(j)$ を生成し (S4)、また乱数生成装置 42 から乱数 $R_i^{(j)}$ を生成し (S5)、更に $b_i^{(j)}$ 生成装置 45 から入札価格 PR_i に応じて価格選択有無情報 $b_i^{(j)}$ を生成する (S6)。 $(+)$ 演算装置 46 はこれら $f(j)$ 、 $R_i^{(j)}$ 、 $b_i^{(j)}$ を入力して $f(j)(+) b_i^{(j)} (+) R_i^{(j)}$ を演算する (S7)。 $(+)$ は適当の演算を示す。この演算結果を一方向性関数 h 処理装置 43 で処理して $h(f(j)(+) b_i^{(j)} (+) R_i^{(j)})$ を生成する (S8)。次に j を +1 してステップ S3 に戻る (S9)。 j が n を換え、全ての j について

の処理が終ると、入札装置 11_i から識別子 ID_i と、入札指標 {h (f (1) (+) b_i⁽¹⁾ (+) R_i⁽¹⁾), ..., h (f (n) (+) b_i⁽ⁿ⁾ (+) R_i⁽ⁿ⁾)} を出力する (S10)。

【0062】

このように一方向性関数を用いて各価格に対する入札指標を作成し、全指標を出力することにより、本命の入札価格を秘密にできることができる。

このような入札データを入力して開札処理を行う開札装置 12 は図 26 に示すように制御装置 21、一方向性関数 h 処理装置 22、関数 f 処理装置 26、減算器 24、メモリ手段 35、および他の装置からも参照可能な共有記録媒体 25、(+) 演算装置 51 から成る。

【0063】

この開札装置 12 の動作は図 27 に示すように、 $1 \leq i \leq m$ という i に対して、{ID_i, h (f (1) (+) b_i⁽¹⁾ (+) R_i⁽¹⁾), h (f (2) (+) b_i⁽²⁾ (+) R_i⁽²⁾), ..., h (f (n) (+) b_i⁽ⁿ⁾ (+) R_i⁽ⁿ⁾)} が入力され、これらを共有記録媒体 25 に蓄積する (S1)。価格パラメータ k をその最高値 n とする (S2)。全入札装置 11_i に R_i^(k) の提示を要求する (S3)。各入札装置 11_i は各々 R_i^(k) を開札装置 12 に入力する。開札装置 12 はその全ての R_i^(k) を共有記録媒体 25 に蓄積する (S4)。開札装置 12 は b_i^(k) = 1 とし、関数 f 処理装置 26 で f (k) を求め、この f (k) と b_i^(k) = 1 と R_i^(k) を (+) 演算装置 51 に入力して、f (k) (+) 1 (+) R_i^(k) を演算し、その結果を一方向性関数 h 処理装置 22 で処理して h (f (k) (+) 1 (+) R_i^(k)) を求める。各 i に対して h (f (k) (+) 1 (+) R_i^(k)) が共有記録媒体 25 上にあるかどうかを検証する (S5)。もしなければ k ← k - 1 としステップ S3 に戻る (S6)。ステップ S5 で一致するものがあれば、その k を落札価格 k とし、k と、この落札価格を提示した入札装置 11_i の識別子 ID_i を出力して終了する (S7)。

【0064】

このように一方向性関数を用いて各価格に対する入札指標を作成し、かつ全指標を開札対象とし、最高値から順にオープンすることにより非落札価格を秘密に

できる。

この実施例 5 において最低入札価格を落札価格とする場合は、入札装置 11_i から同様に $\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ を開札装置へ送る。開札装置 12 では図 27 に示した処理とほぼ同様に処理するが、ステップ S2 では入札可能な n 種類の価格の最低値 1 を k にセットし、ステップ S6 では $k \leftarrow k + 1$ とする。その他の処理は同様である。

【0065】

この実施例 5 において最高価格を入札価格とする場合は $n \leq k' \leq k$ なる k' について $R_i^{(k')}$ が共有記録媒体 25 に記録されているから、その落札価格 k が正しいものであるかを、誰でもが調べることができる。

この実施例 5 において、乱数 $R_i^{(j)}$ が入札装置 11_i 自身の他に開札装置 12 も知っているようにすることもできる。その場合の開札装置 12 の処理を図 28 に示す。

【0066】

各入札装置 11_i から、 $1 \leq i \leq m$ という i に対して、 $\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \dots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$ が入力され、これらを共有記録媒体 25 に蓄積する (S1)。価格パラメータ k を取り得る最高値 n とする (S2)。開札装置 12 は全ての i に対して、 $b_i^{(k)} = 1$ として $h(f(k)(+)1(+)R_i^{(k)})$ を作成し、この値が共有記録媒体 25 上に一致するものが存在するかを検証する (S3)。一致するものがなければ $k \leftarrow k - 1$ としてステップ 3 に戻る (S4)。一致するものが $k' \geq h$ である全ての $R_i^{(k')}$ を共有記録媒体 25 に蓄積し (S5)、この時の k を落札価格とし、この k と、この落札価格を提示した入札装置 11_i の識別子 ID_i を出力して終了する (S6)。

【0067】

この場合で最低入札価格を落札価格とする場合は、図 28 において、ステップ S2 で、k を、取り得る価格の最小値、この例では 1 とし、ステップ S4 では k

を+1とし、ステップS5では $k' \leq k$ である全ての $R_i^{(k')}$ を共有記録媒体25に蓄積する。その他は図28の処理と同様である。

仮識別子装置を用いた電子競争入札装置

図29に仮識別子装置を用いた電子競争入札装置を示す。

【0068】

各入札装置11_iは仮識別子登録装置52と通信することができるようになっている。

この電子競争入札装置の動作は図30に示すように行われる。

Step 1: 入札装置11_iは外部から入力された入札公告を受けて、識別子ID_iを出力し、仮識別子登録装置52へ入力する。

Step 2: 仮識別子登録装置52は入力されたID_iに対して、仮識別子であるAID_iを発行し、記録媒体53にID_iとAID_iを組にして保存し、AID_iを入札装置11_iへ返す。

Step 3: 入札装置11_iは入札価格PR_iを生成し、

Step 4: その入札価格を入札指標 γ_i に変換し、

Step 5: 入札装置11_iは入札指標 γ_i とAID_iを出力し、開札装置12へ入力する。

Step 6: 開札装置12は全入札指標から落札価格を求め、

Step 7: 落札価格と、この落札価格を提示した入札装置の仮識別子を出力する。

【0069】

このようにして誰れが入札へ参加したかを秘密にしておくことができる。なお開札装置12は仮識別子登録装置52に問い合わせ、落札価格と対応する仮識別子がAID_iから識別子ID_iを知ることができる。

上述において $f(PR_i)$ は単調増加かつ正整数を出力する関数であるが、 $f(PR_i) = PR_i$ も含むものである。 $f(n, PR_i)$ は例えば $n - PR_i$ である。入札装置11_iや開札装置12はその機能をコンピュータによりプログラムを解読実行させることにより作用させることもできる。

【0070】

【発明の効果】

以上述べたようにこの発明によれば、入札価格を、一方向性関数を利用して入札指標に変換して、開札装置へ送っているため、入札前に各入札装置は他の入札装置の入札価格を知ることができず、公平に入札を行うことができる。

また $h^{f(n+1)}(IV_i)$ や $h^{f(n,q'-1)}(IV_i)$ を全入札装置間に共有させ、落札価格に対応する $h^{f(PRi)}(IV_i)$ や $h^{f(n,PRi)}(IV_i)$ を公開することにより、落札価格が確かに改ざんされることなく、正しくその額で入札されたものであるか否かを、全ての入札装置が検証することができる。

【0071】

またこの発明によれば落札価格以外の入札価格を秘密にしたまま、落札価格を判定することができる。

実施例 2 によれば開札装置にも落札価格以外の入札価格が知れない。

実施例 3 によれば、開札装置にも落札価格以外の入札価格が知れず、しかも、入札装置との通信量を消滅することができる。

【0072】

実施例 4 によれば、入札時には、入札価格が他に知られるおそれがなく、しかも開札時には、直接入札価格から落札価格を簡単に特定でき、かつその落札価格が正しいことを検証することができる。

実施例 5 によれば、一方向性関数により各価格に対する入札指標を作成し、その全ての指標を開札装置へ送ることにより、本命の入札価格を秘密にすることができる。

【図面の簡単な説明】

【図 1】

電子競争入札装置の一般的構成を示すブロック図。

【図 2】

電子競争入札の一般的手順を示す流れ図。

【図 3】

入札指標を生成する入札装置を示すブロック図。

【図 4】

一方向性関数により入札指標を生成する入札装置を示すブロック図。

【図 5】

一方向性関数処理装置による入札価格変換装置の具体例を示すブロック図。

【図 6】

一方向性関数により入札指標を生成する手順を示す流れ図。

【図 7】

実施例 1 の最高入札価格を落札価格とする開札装置 1 2 の機能構成を示すブロック図。

【図 8】

図 7 の開札装置の動作を示す流れ図。

【図 9】

実施例 1 の最低入札価格を落札価格とする場合の入札価格変換装置を示すブロック図。

【図 1 0】

実施例 1 の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 1 1】

図 1 0 の開札装置の動作を示す流れ図。

【図 1 2】

実施例 2 の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 1 3】

図 1 2 の開札装置の動作手順を示す流れ図。

【図 1 4】

実施例 2 の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 1 5】

図 1 4 の開札装置の動作手順を示す流れ図。

【図 1 6】

実施例 3 の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 1 7】

図 1 6 の開札装置の動作手順を示す流れ図。

【図 1 8】

実施例 3 の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 1 9】

図 1 8 の開札装置の動作手順を示す流れ図。

【図 2 0】

実施例 4 の入札装置の例を示すブロック図。

【図 2 1】

実施例 4 の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 2 2】

図 2 1 の開札装置の動作手順を示す流れ図。

【図 2 3】

実施例 4 の最低入札価格を落札価格とする場合の開札装置の動作手順を示す流れ図。

【図 2 4】

実施例 5 の入札装置の機能構成を示すブロック図。

【図 2 5】

図 2 4 の入札装置の動作手順を示す流れ図。

【図 2 6】

実施例 5 の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図 2 7】

図 2 6 の開札装置の動作手順を示す流れ図。

【図 2 8】

実施例 5 の変形における開札装置の動作手順を示す流れ図。

【図 2 9】

仮識別子を用いた電子競争入札装置を示すブロック図。

【図 3 0】

図 2 9 の装置の入札手順を示す流れ図。

【書類名】 図面

【図 1】

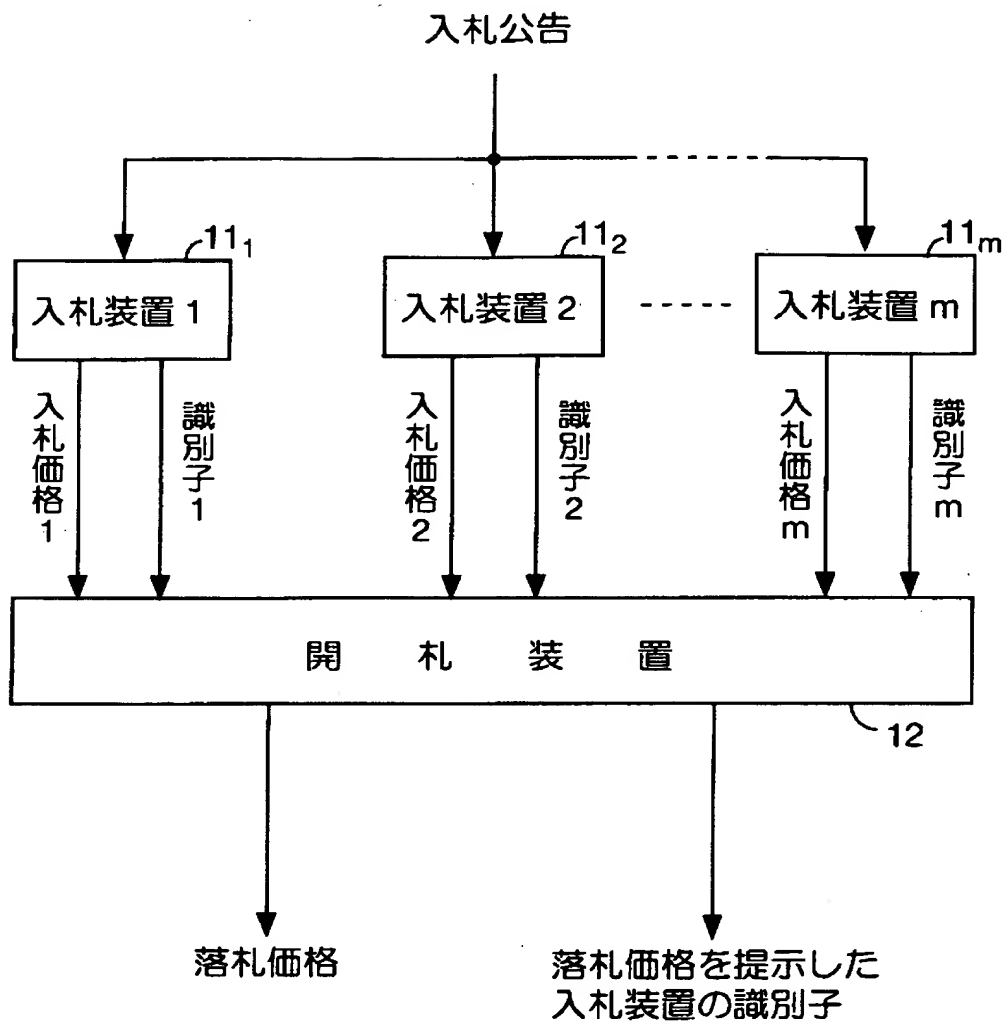


図 1

【図 2】

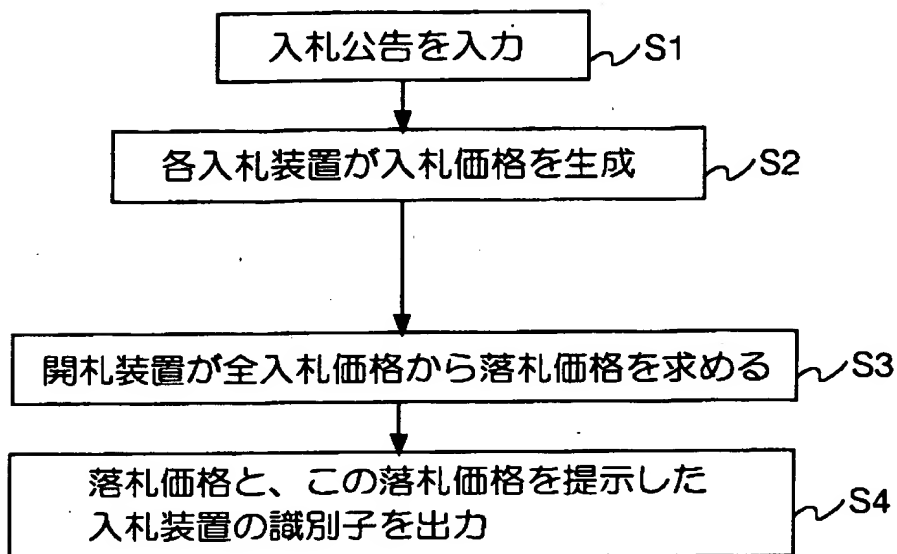


図 2

【図 3】

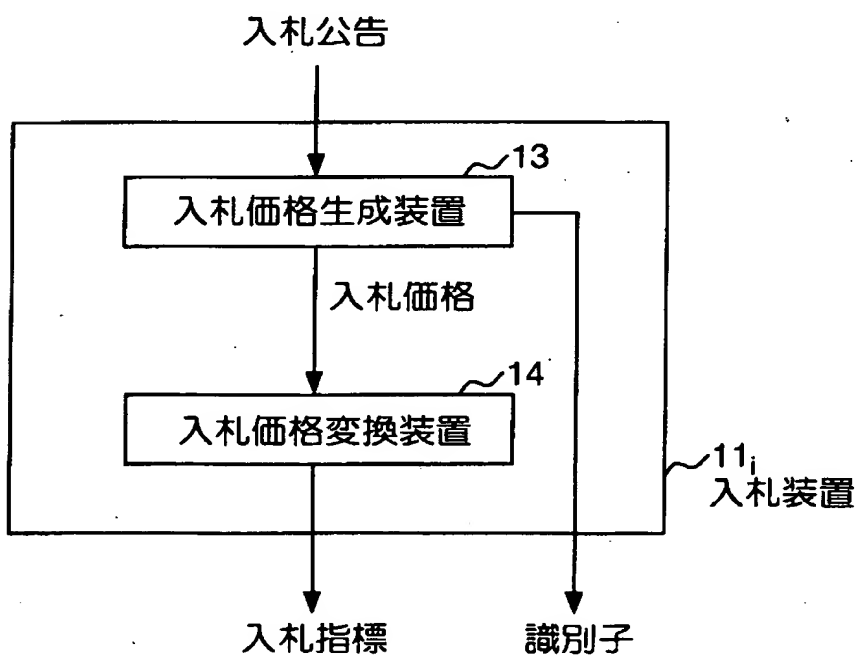
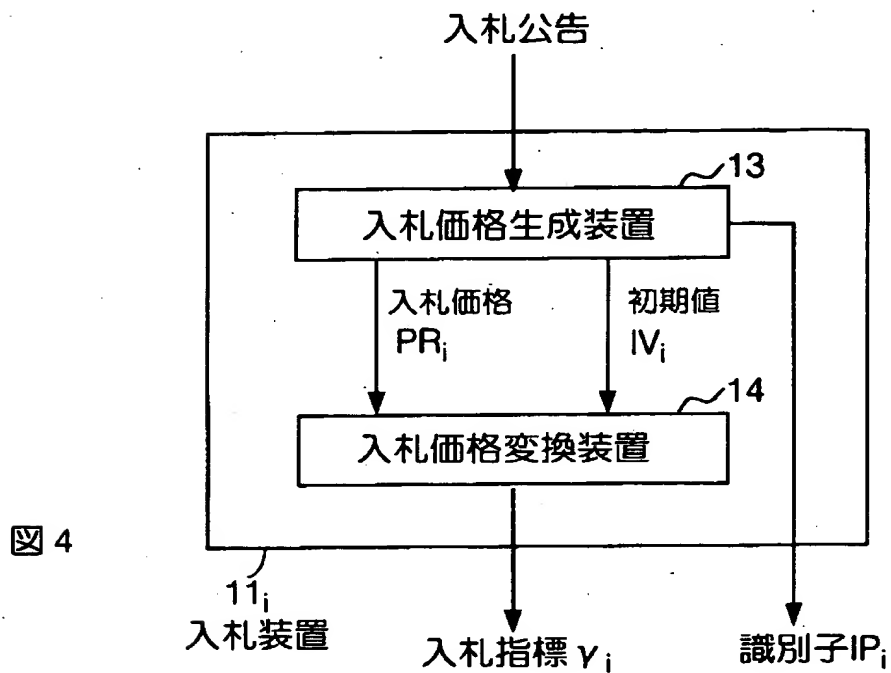
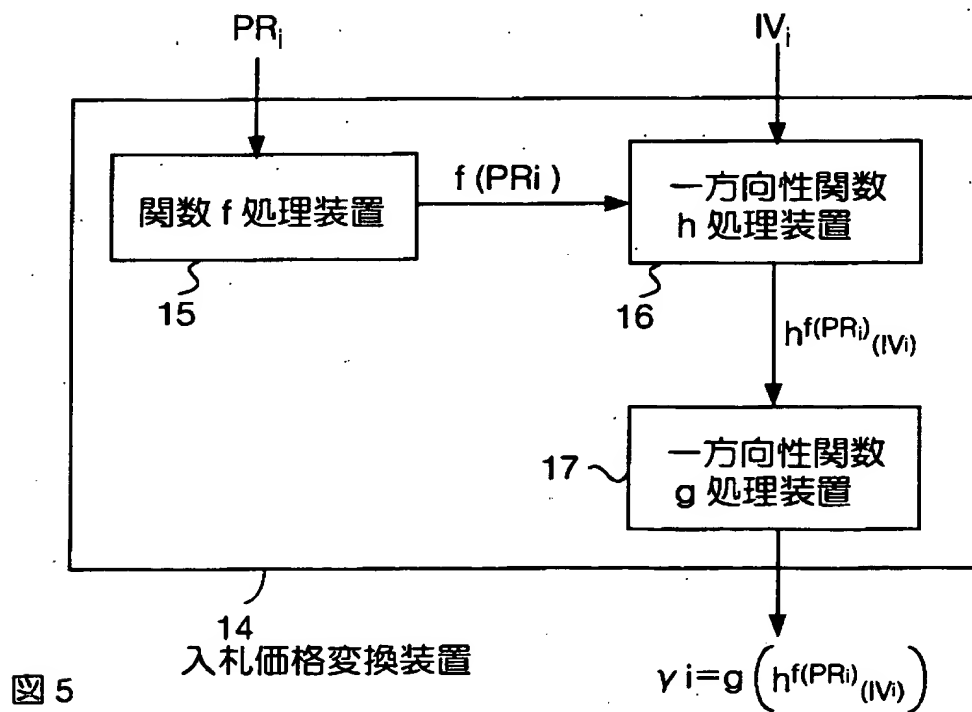


図 3

【図 4】



【図 5】



【図 6】

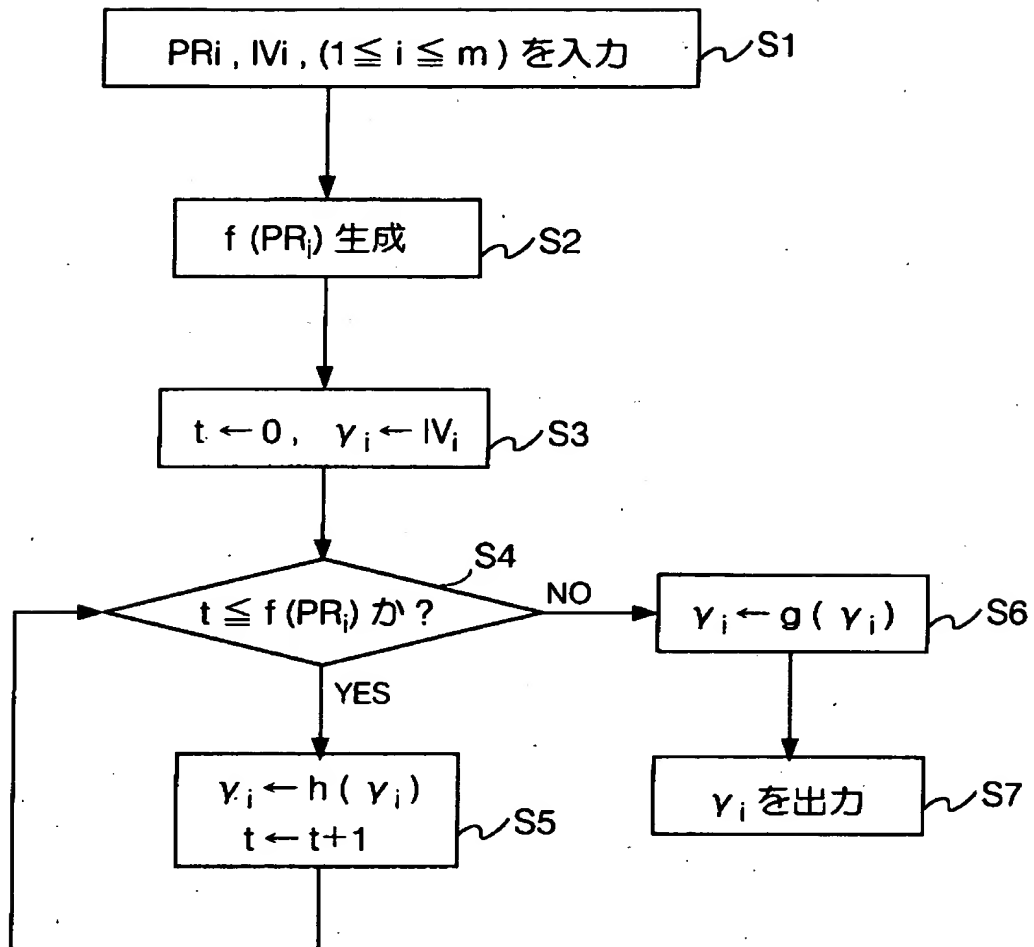
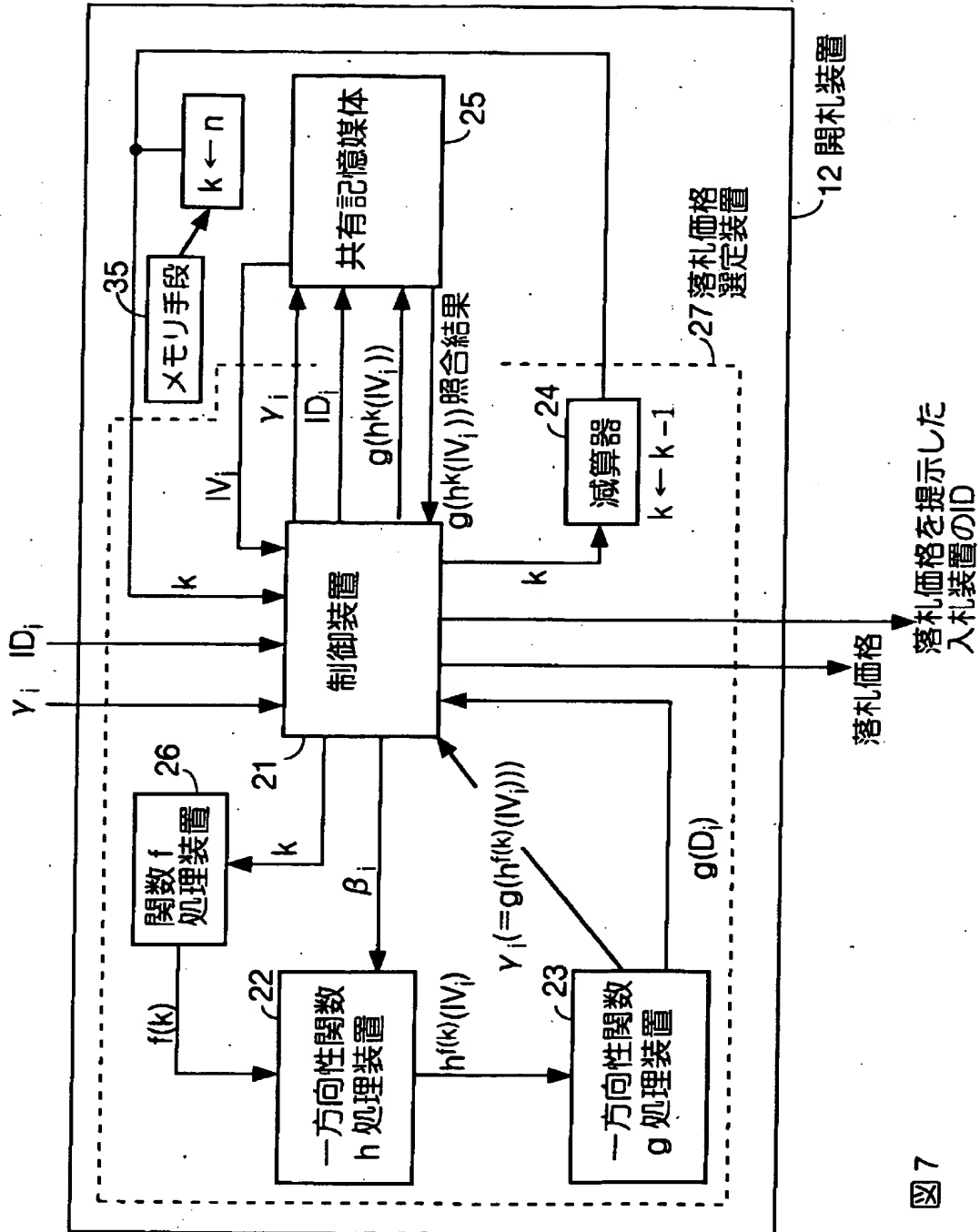


図 6

【図 7】



【図 8】

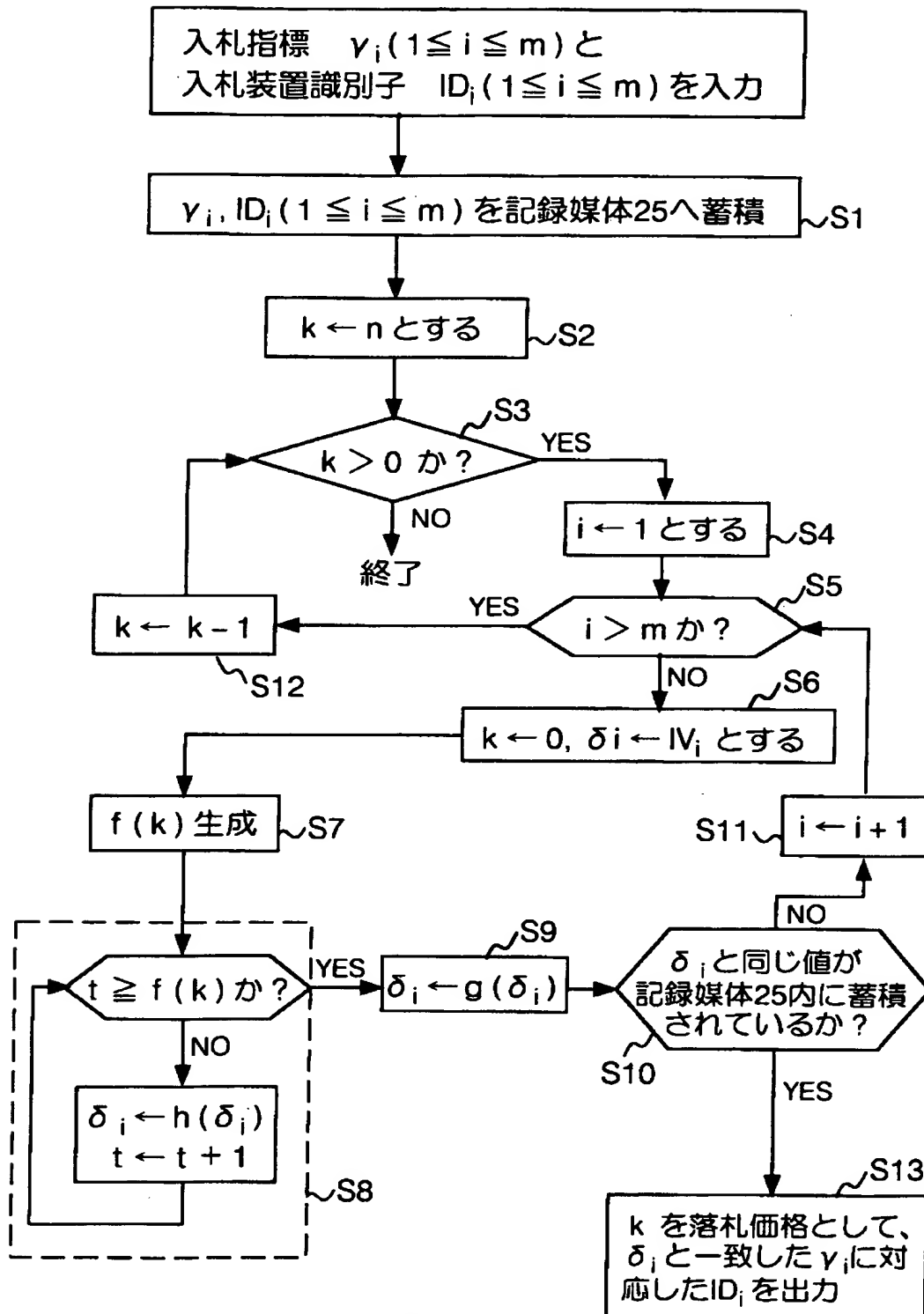


図 8

【図 9】

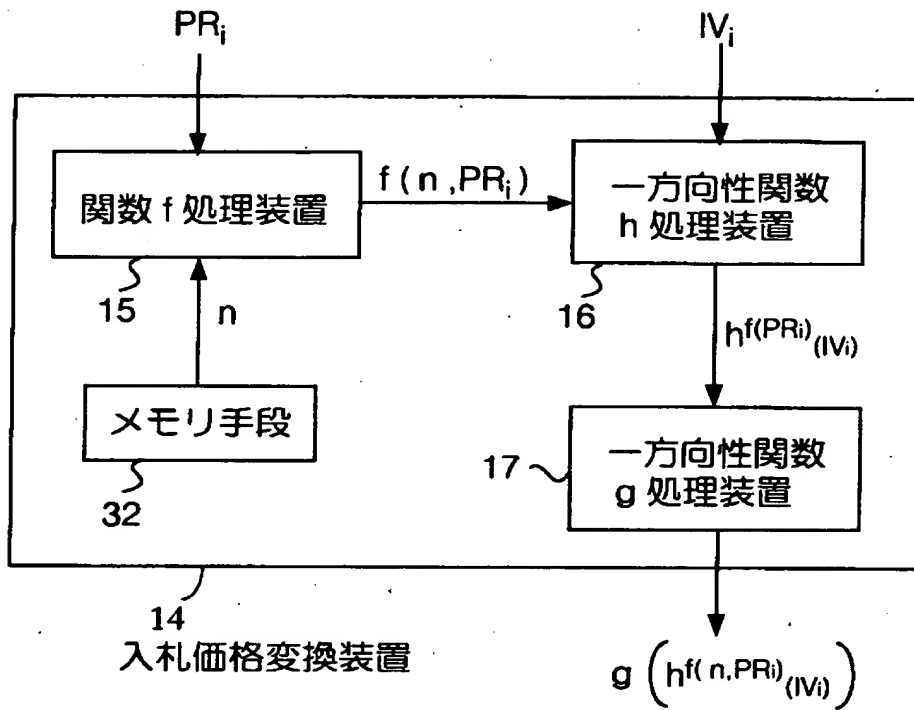


図 9

【図 10】

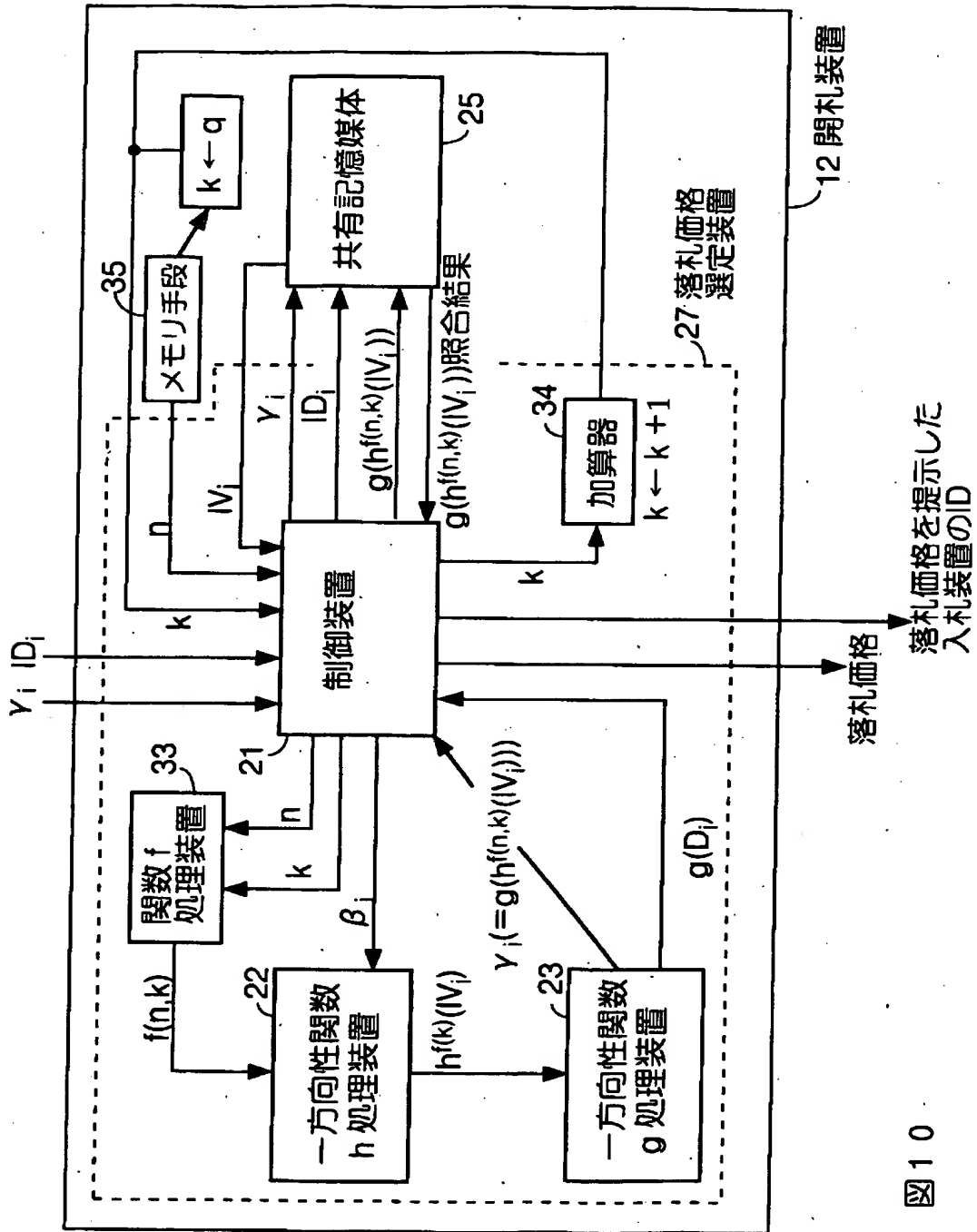


図 10

【図 11】

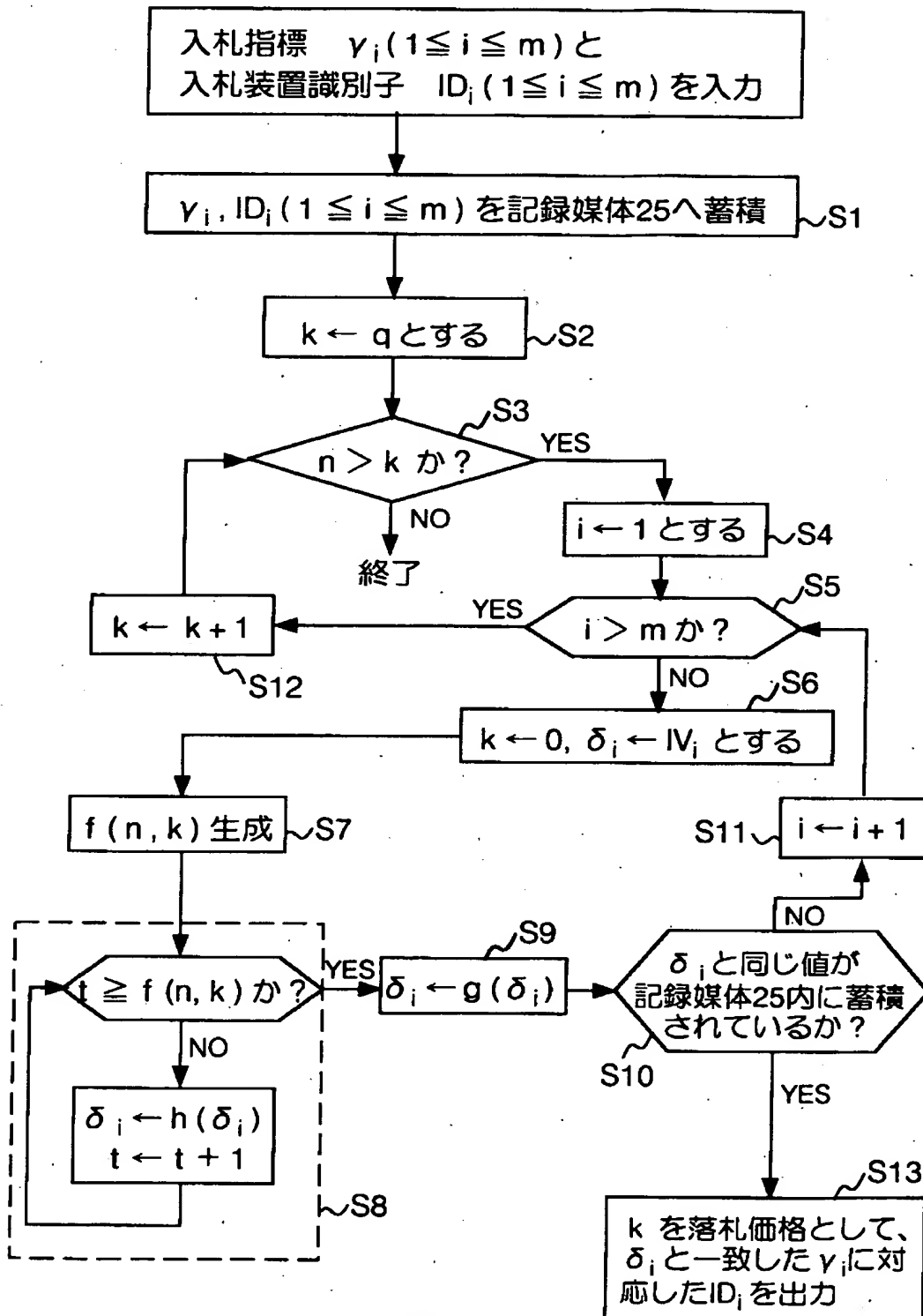


図 11

【図 1 2】

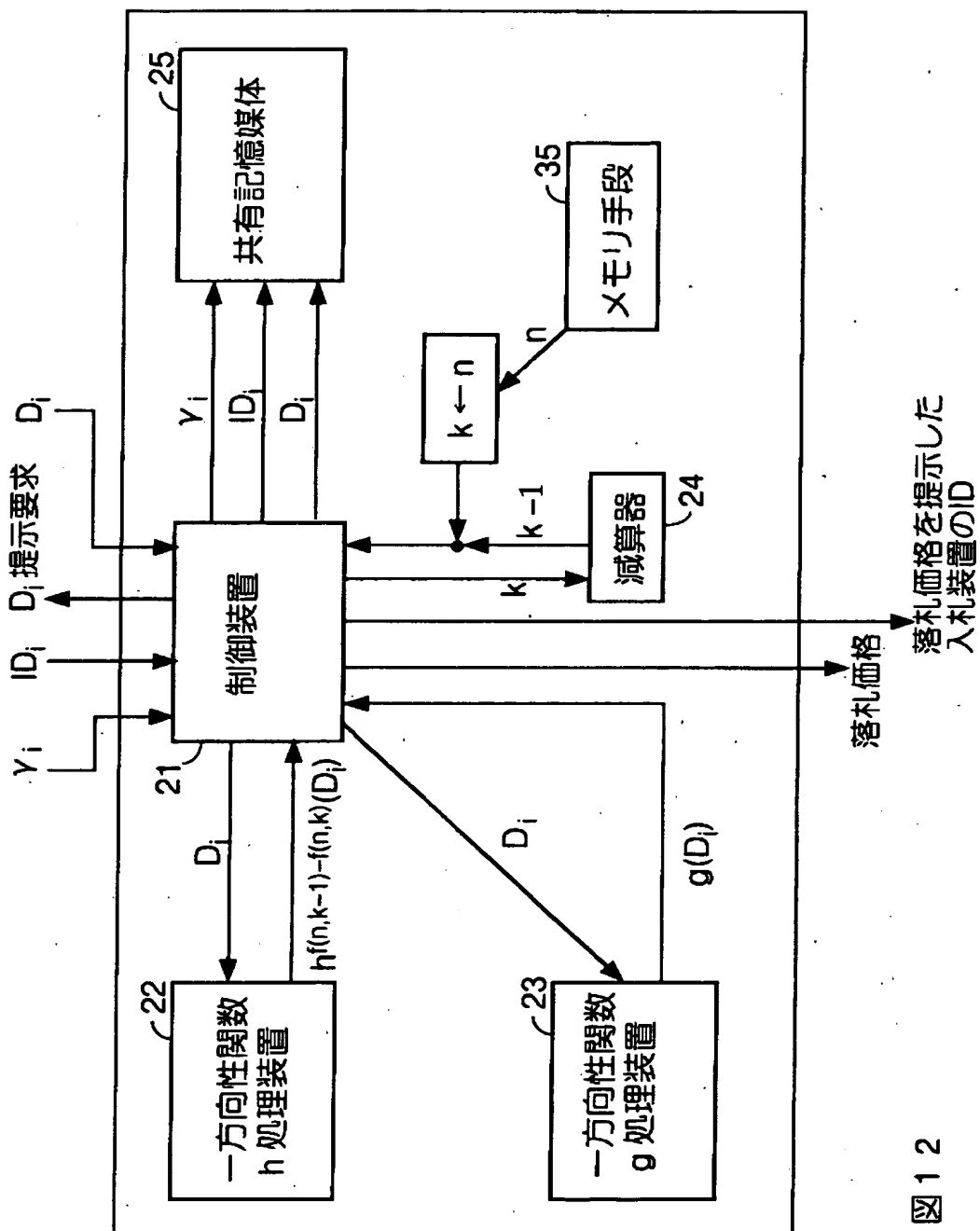


図 1 2

【図 13】

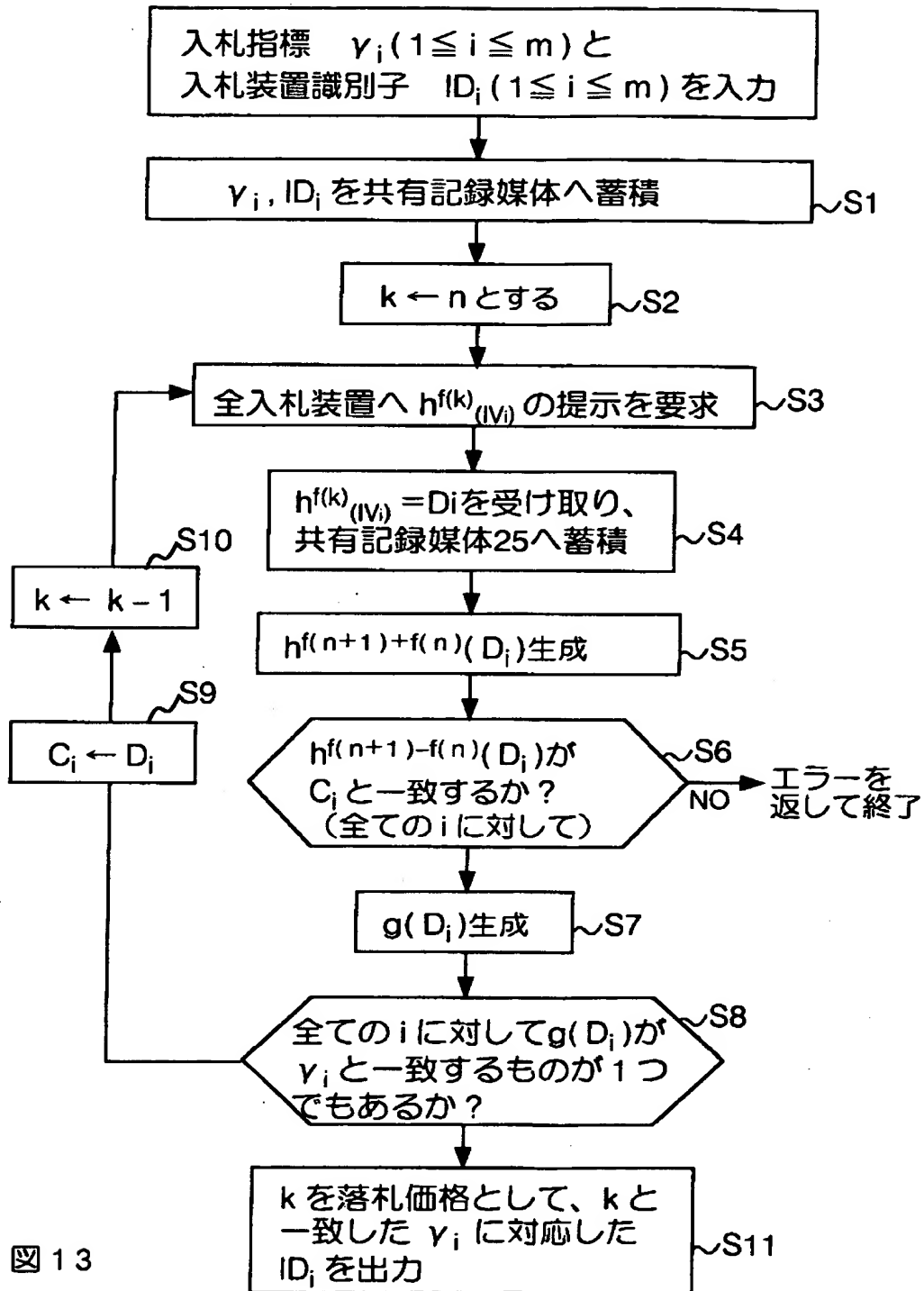


図 13

【図 14】

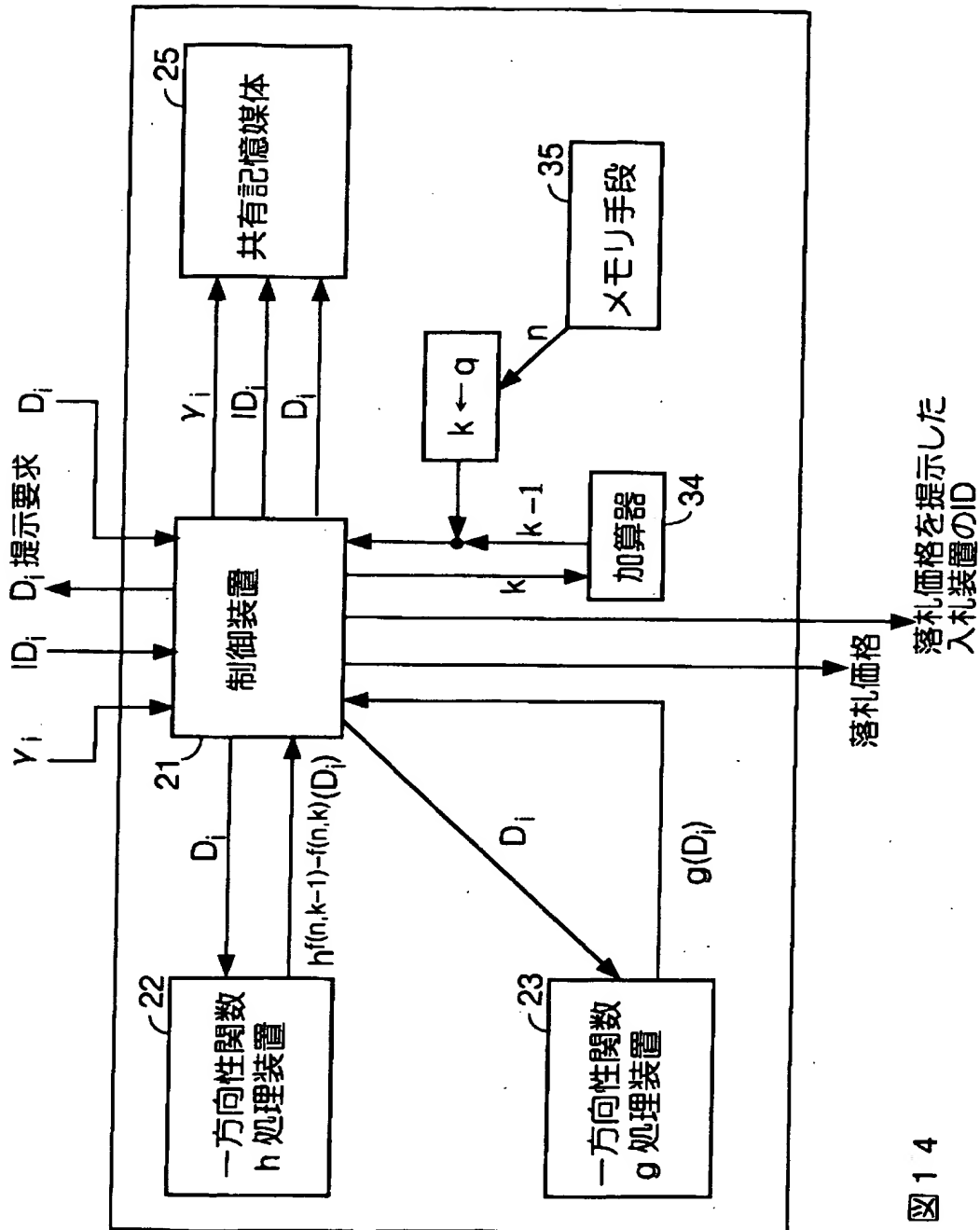


図 14

【図 15】

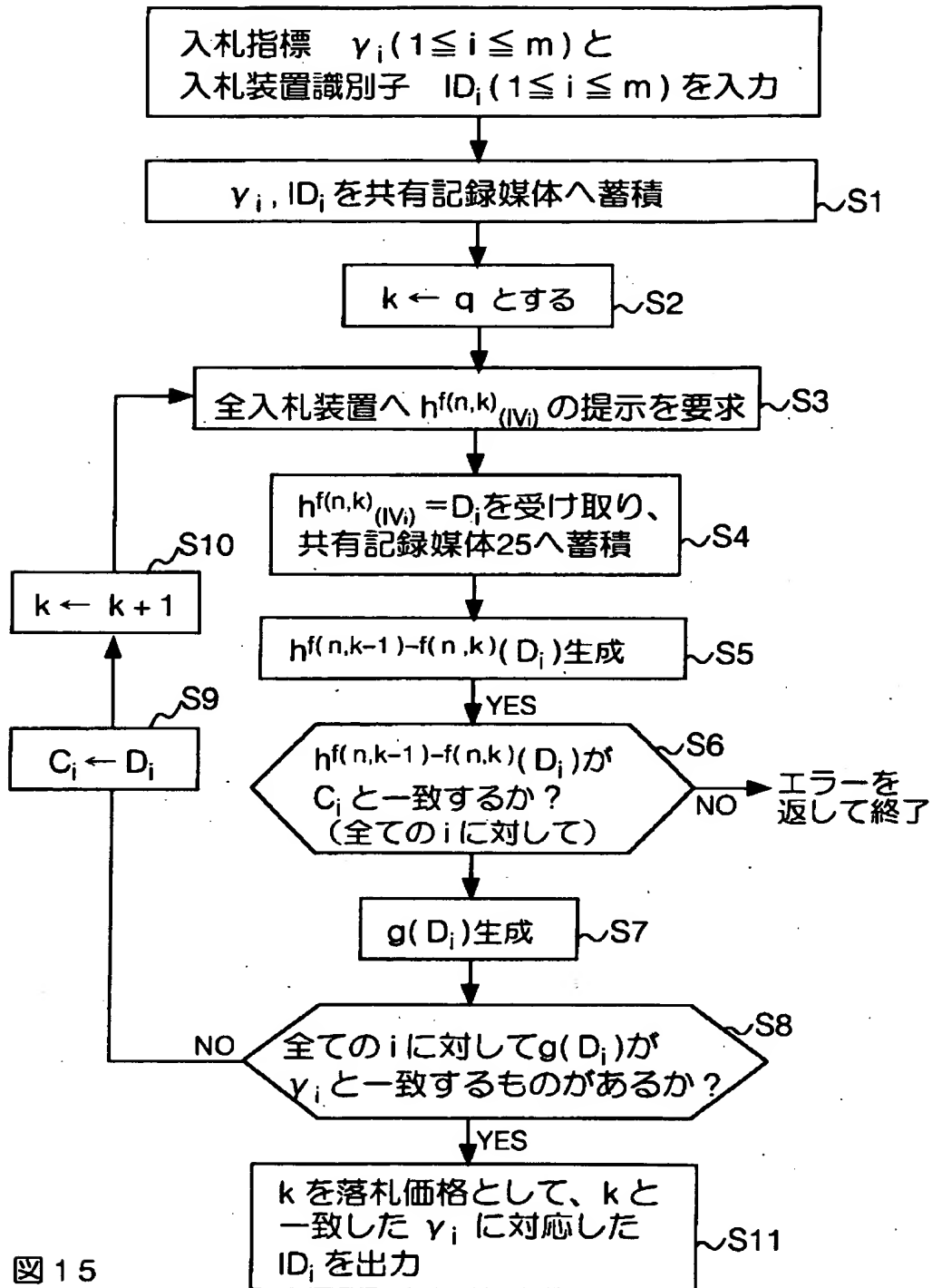


図 15

【図 1 6】

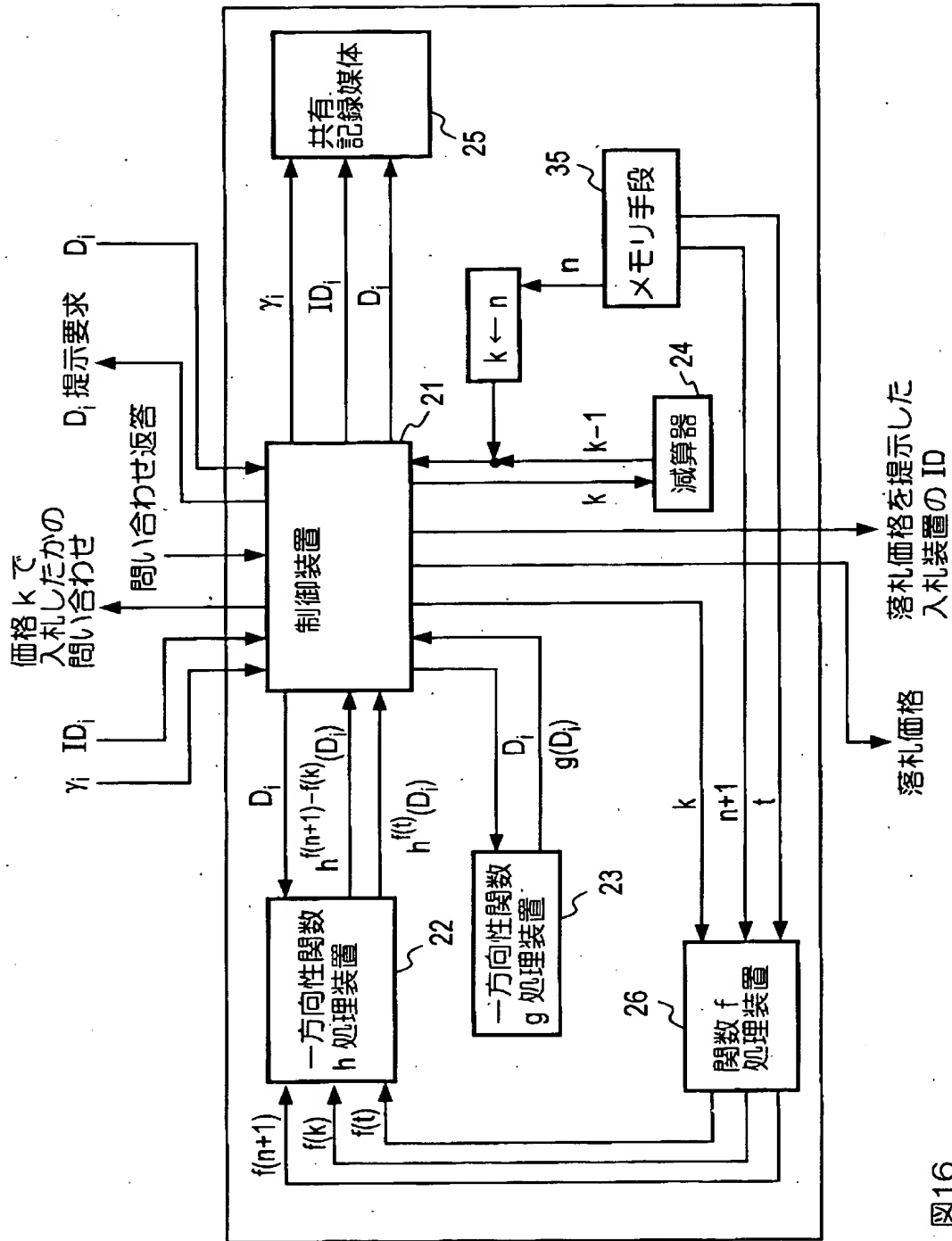


図16

【図 17】

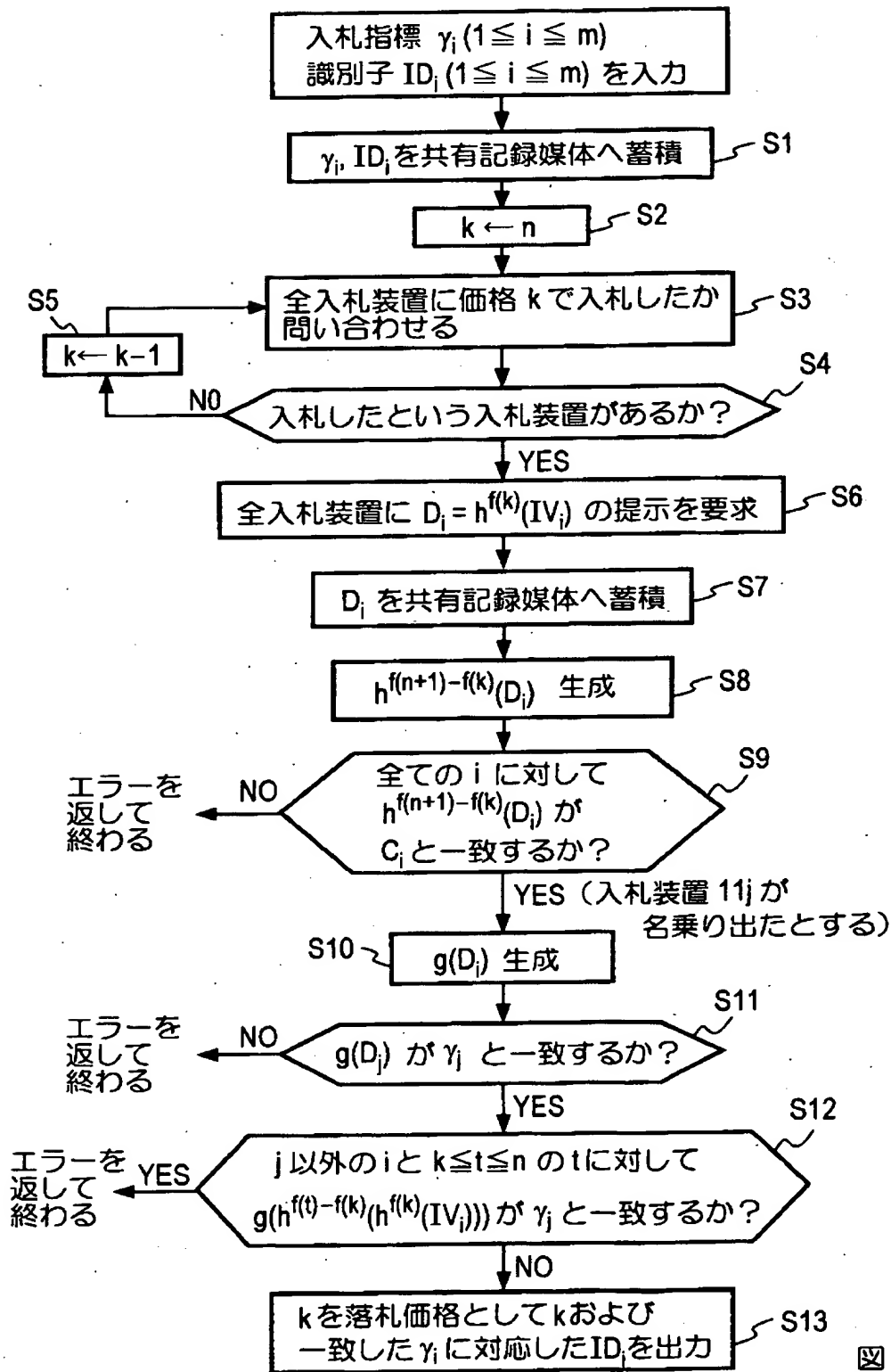


図 17

【図 1 8】

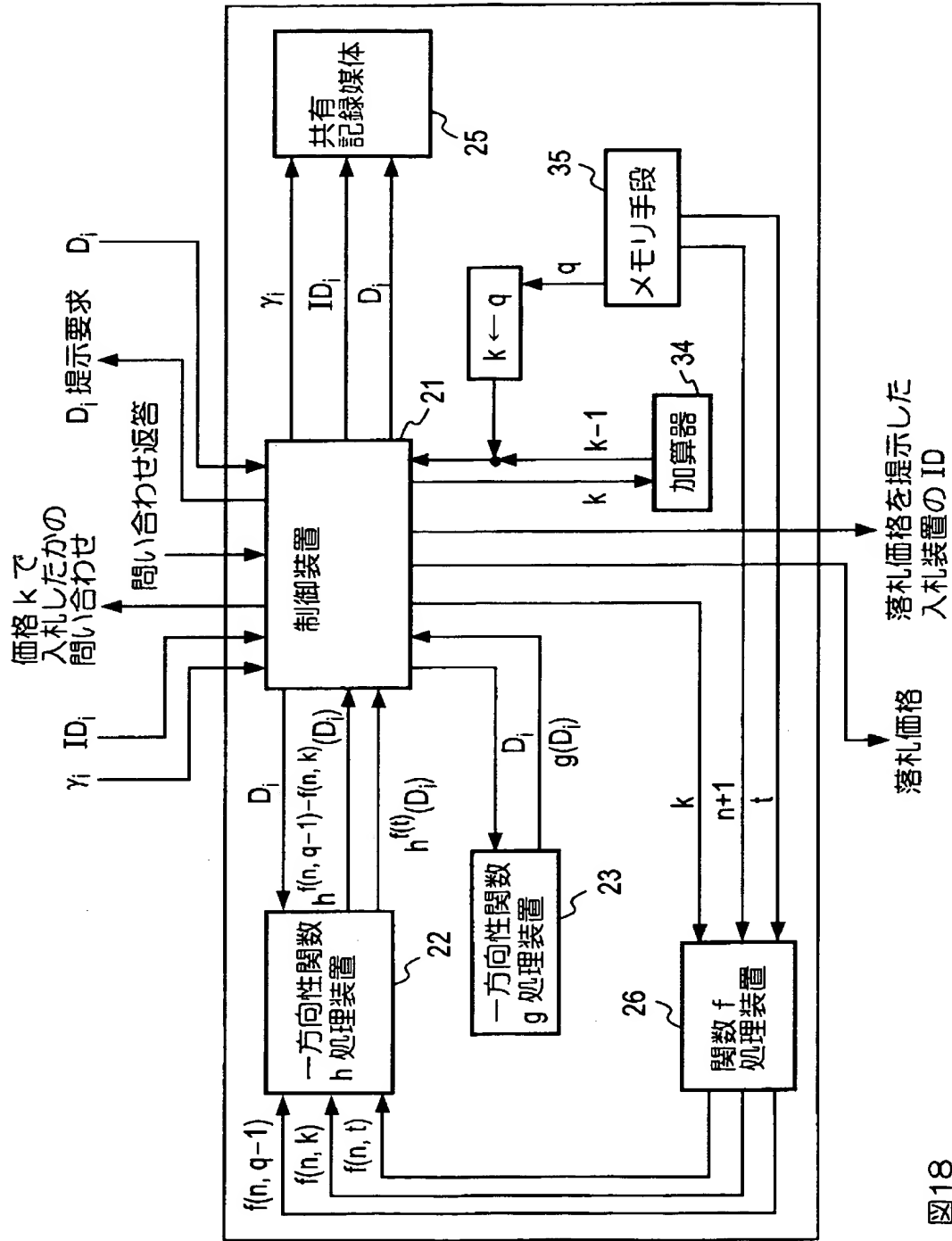


図18

【図 19】

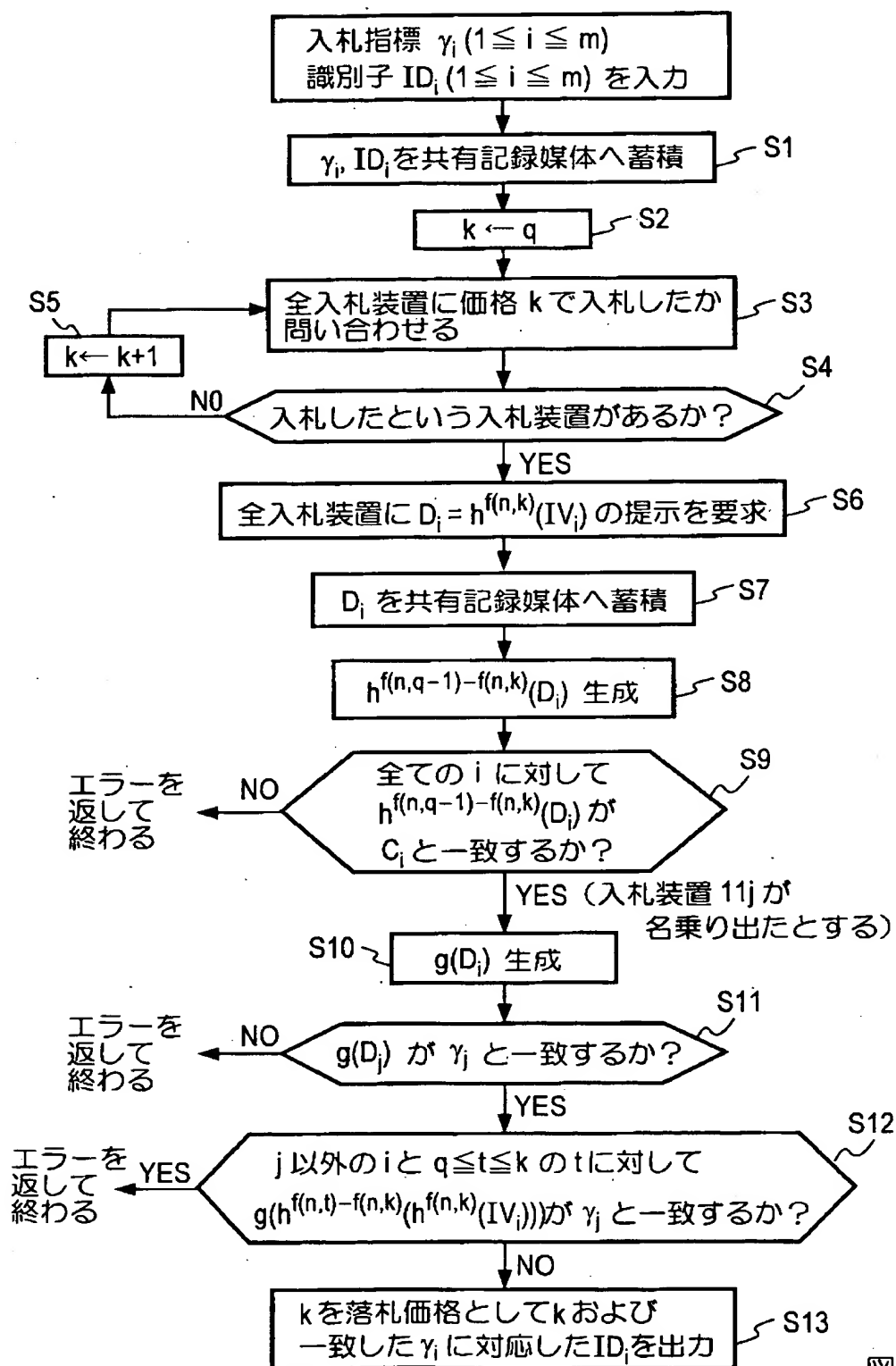


図 19

【図 2 0】

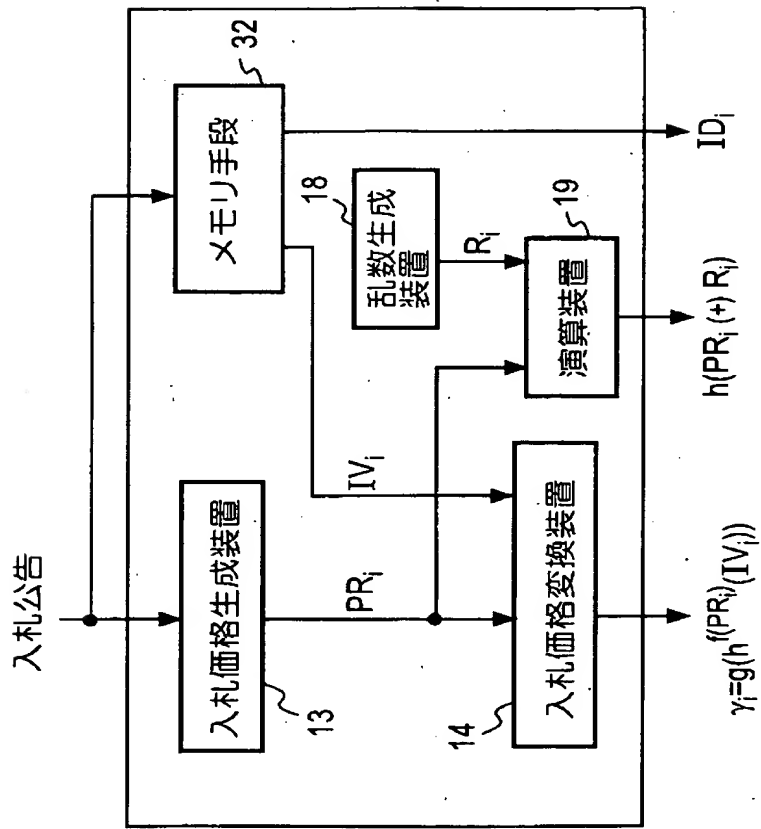


図 20

【図 2 1】

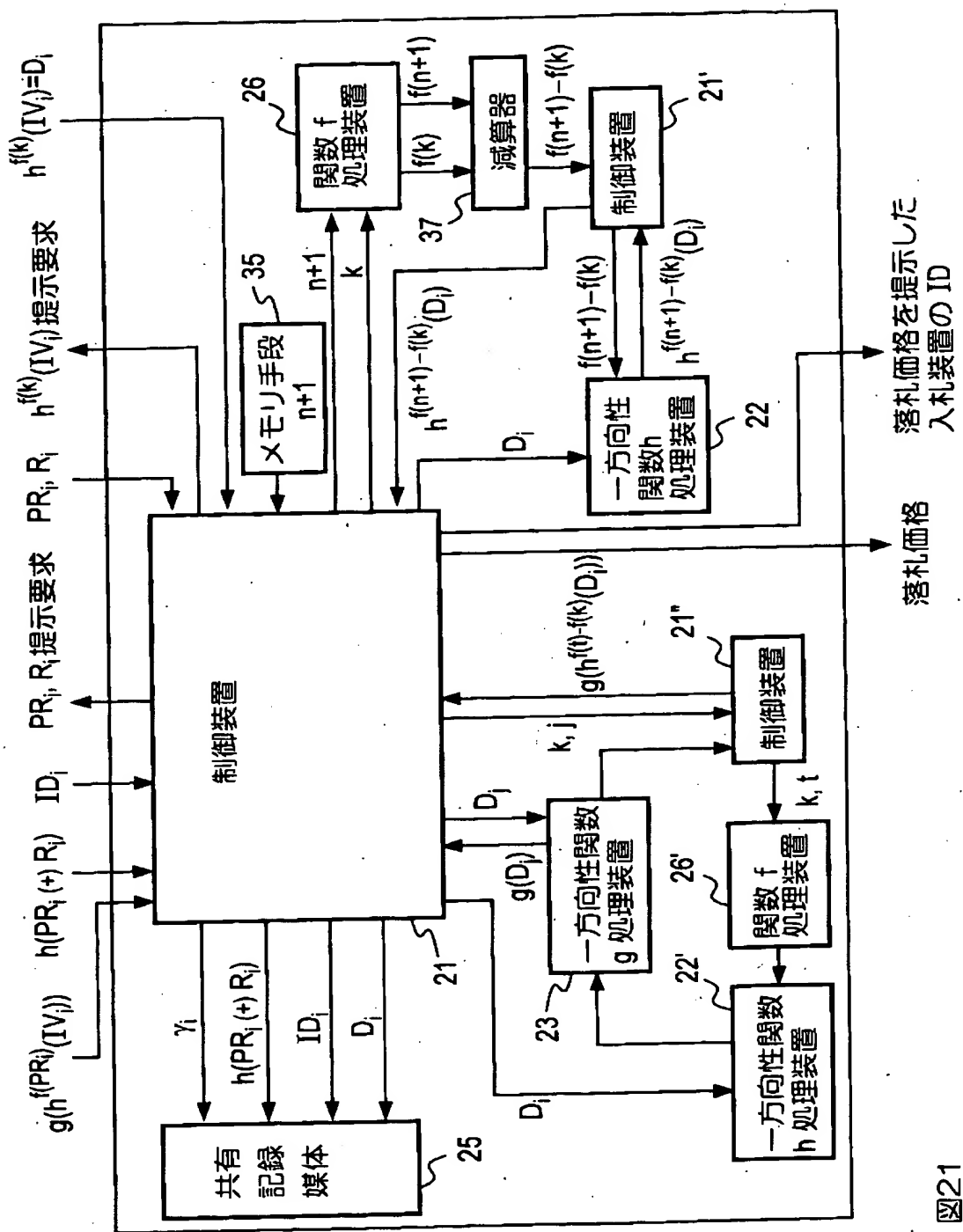


図21

【図 22】

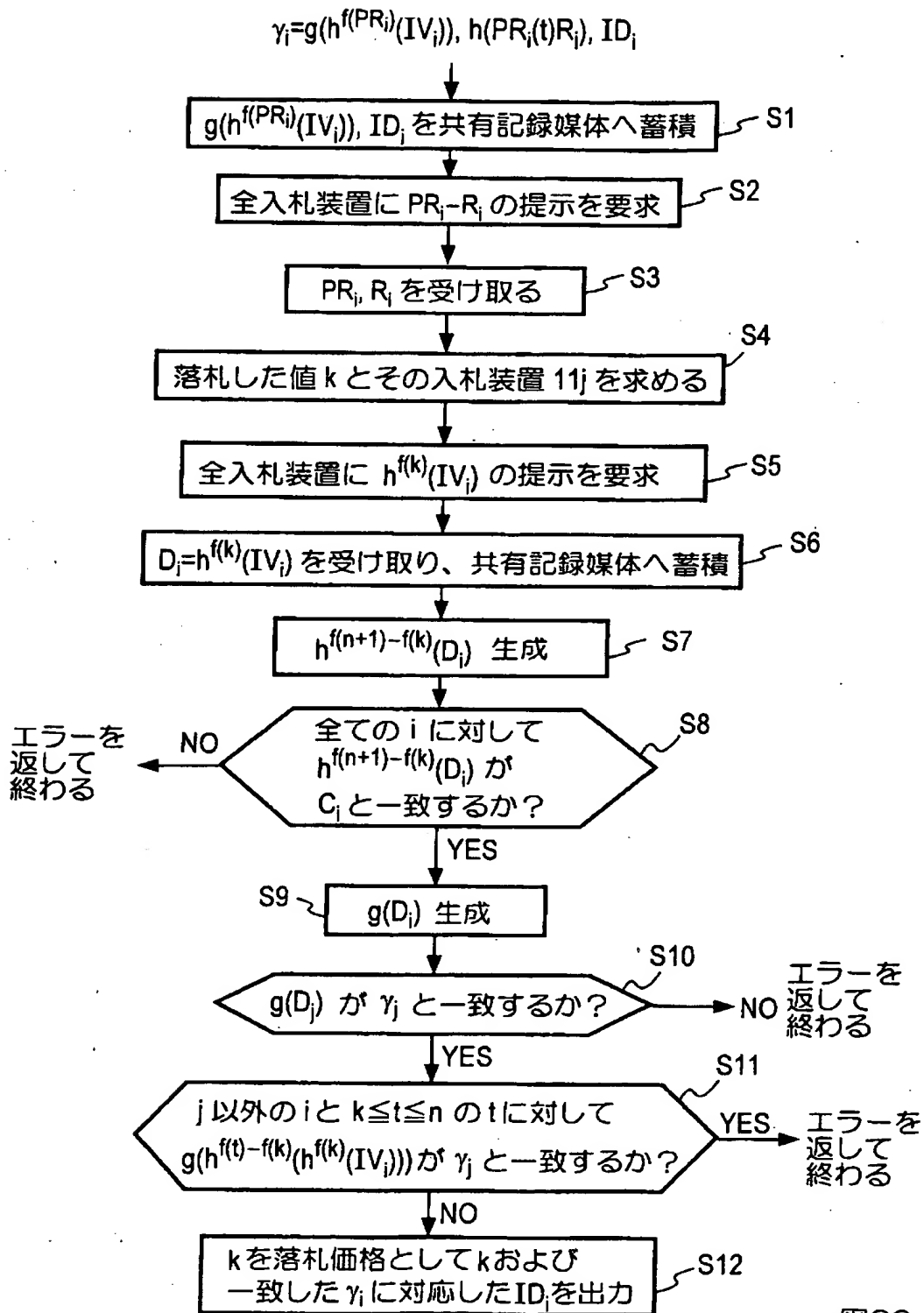


図22

【図 23】

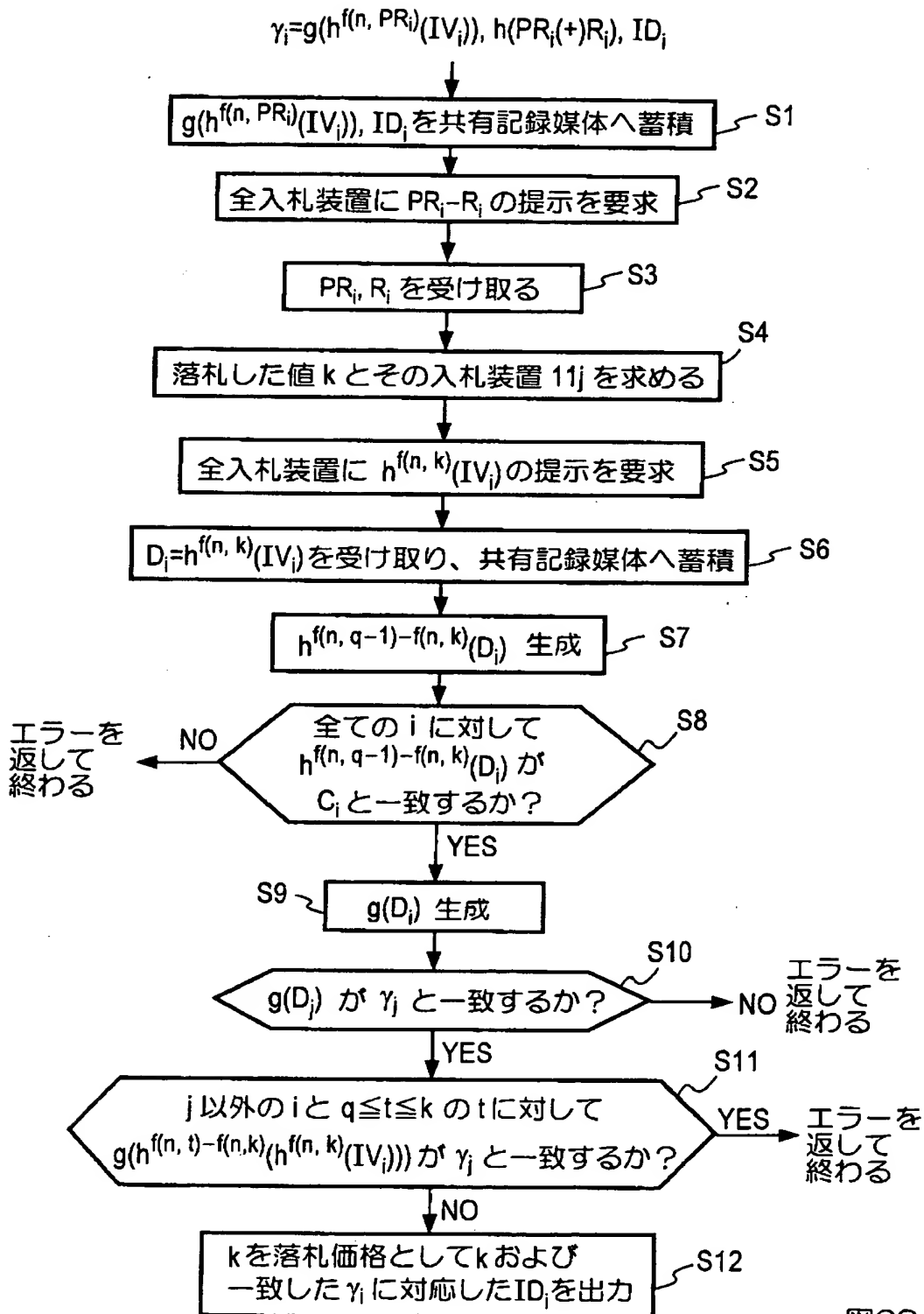


図23

【図 24】

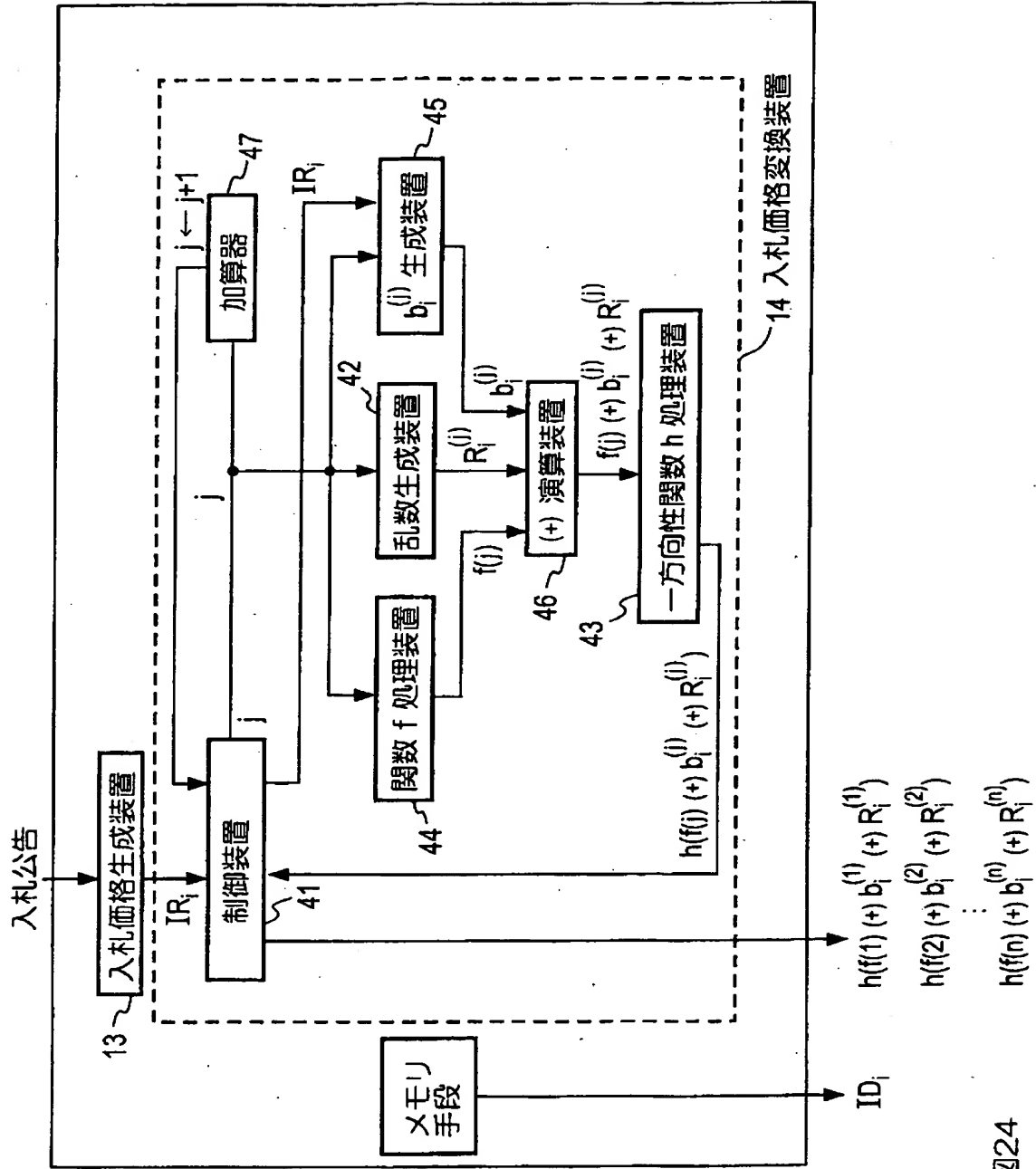


図24

【図 2 5】

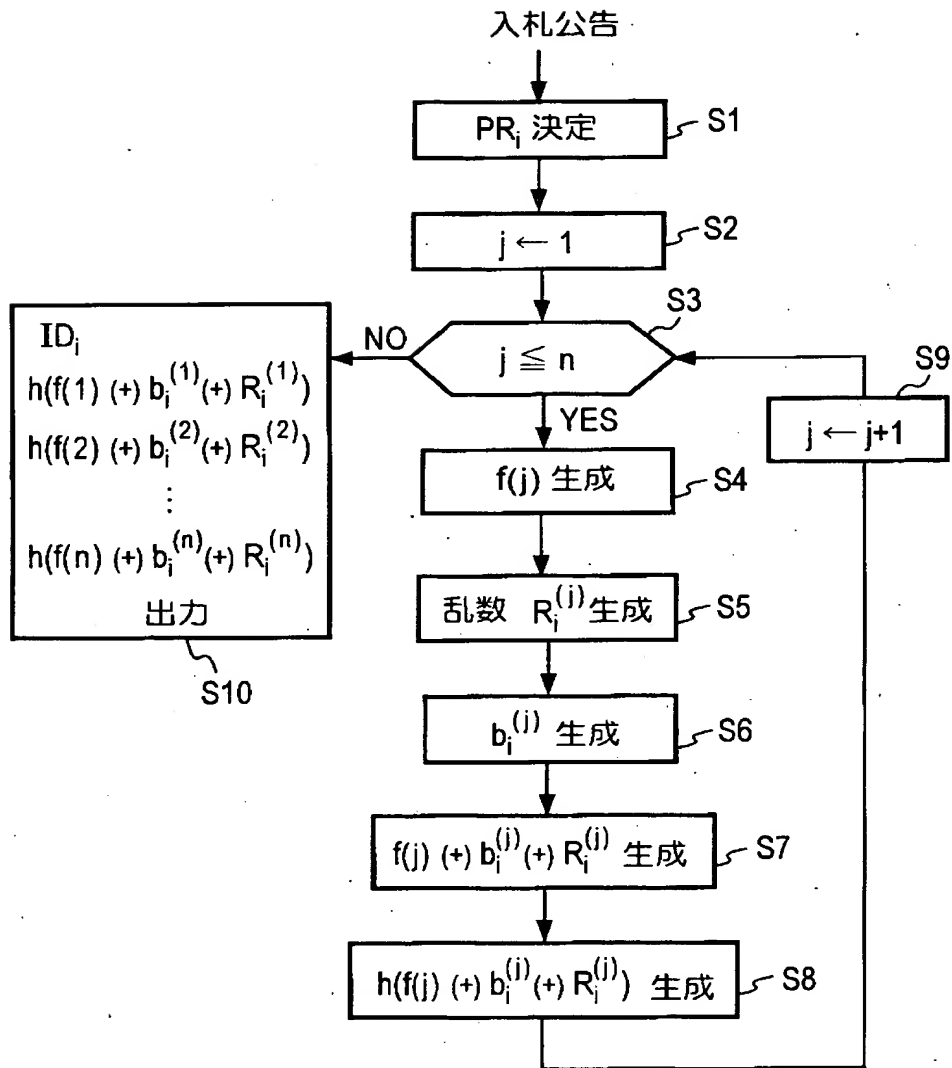


図25

【図 2 6】

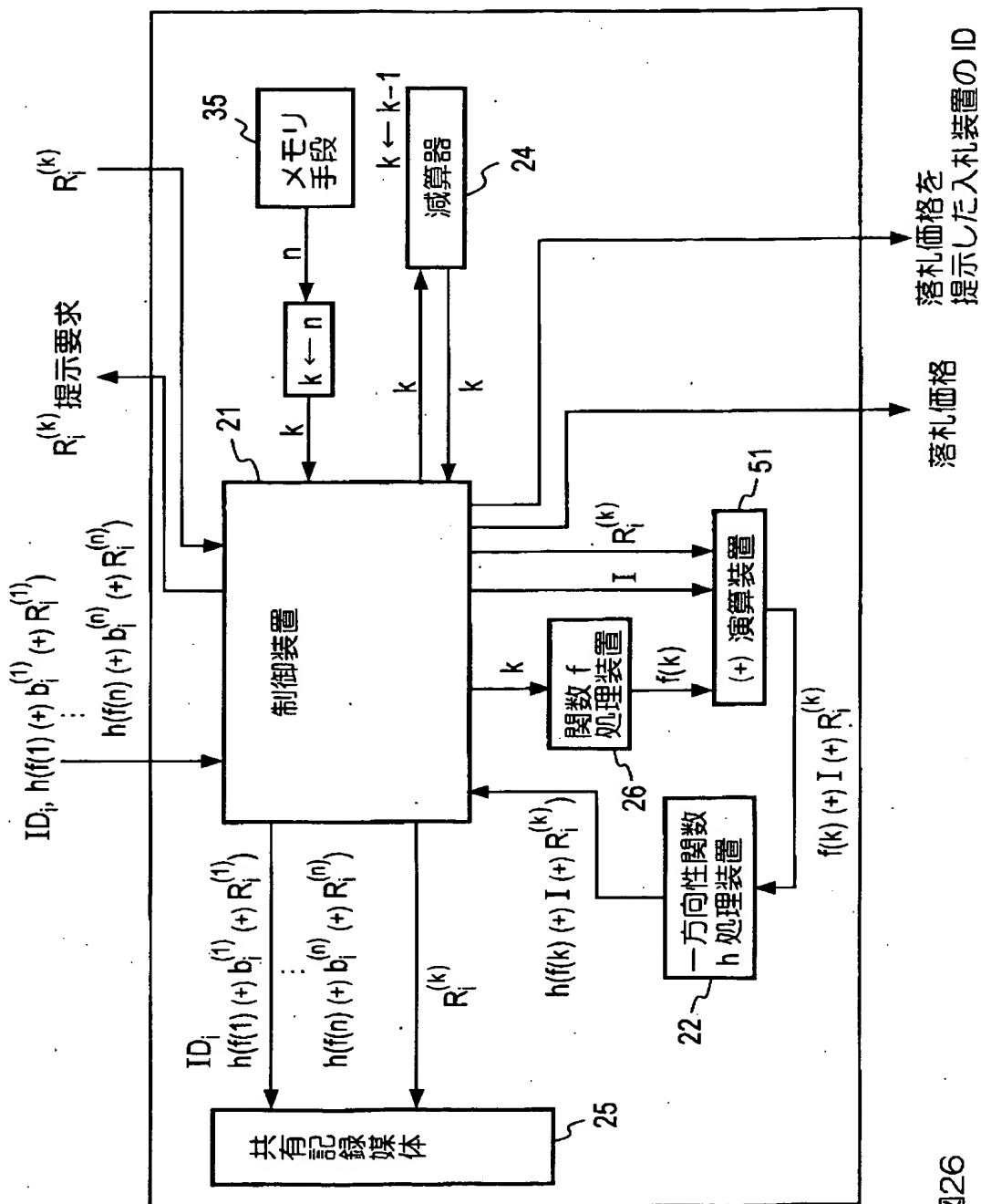


図26

【図 2 7】

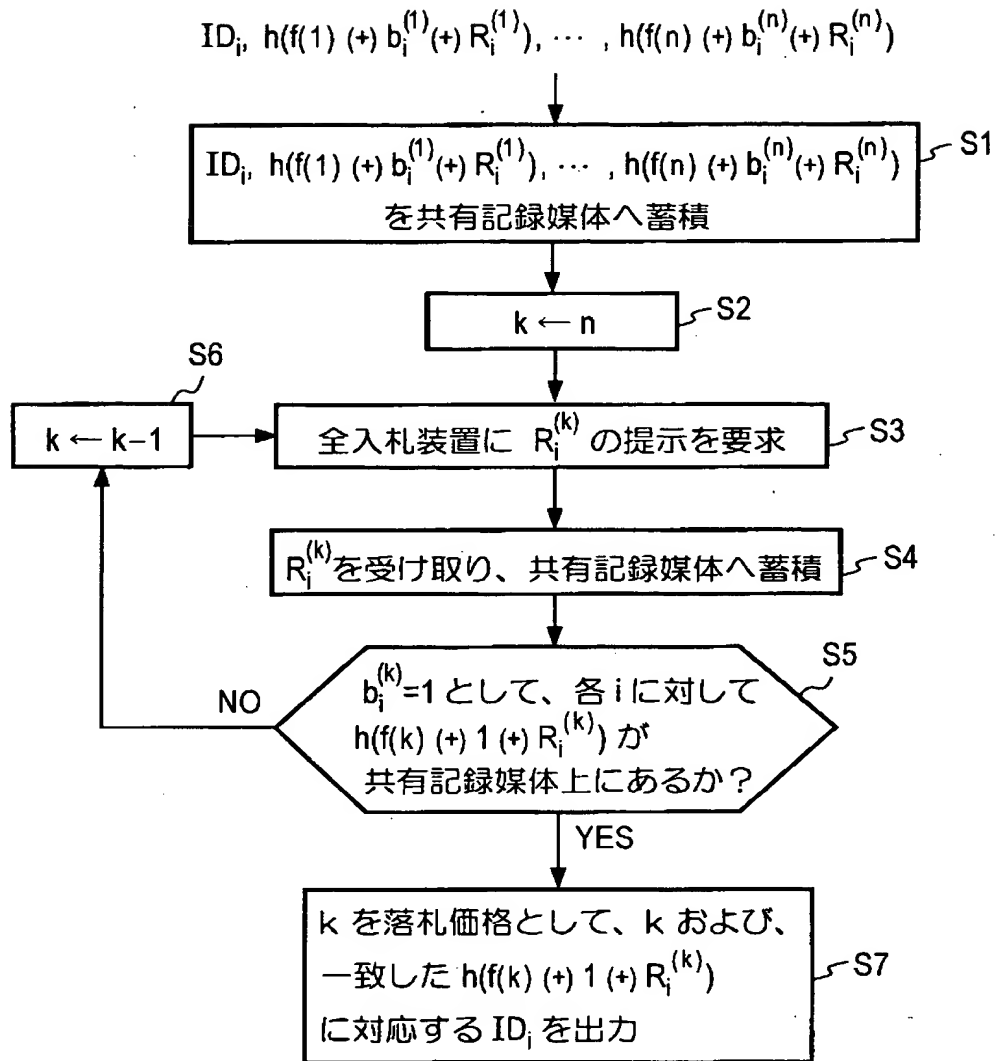


図27

【図 2 8】

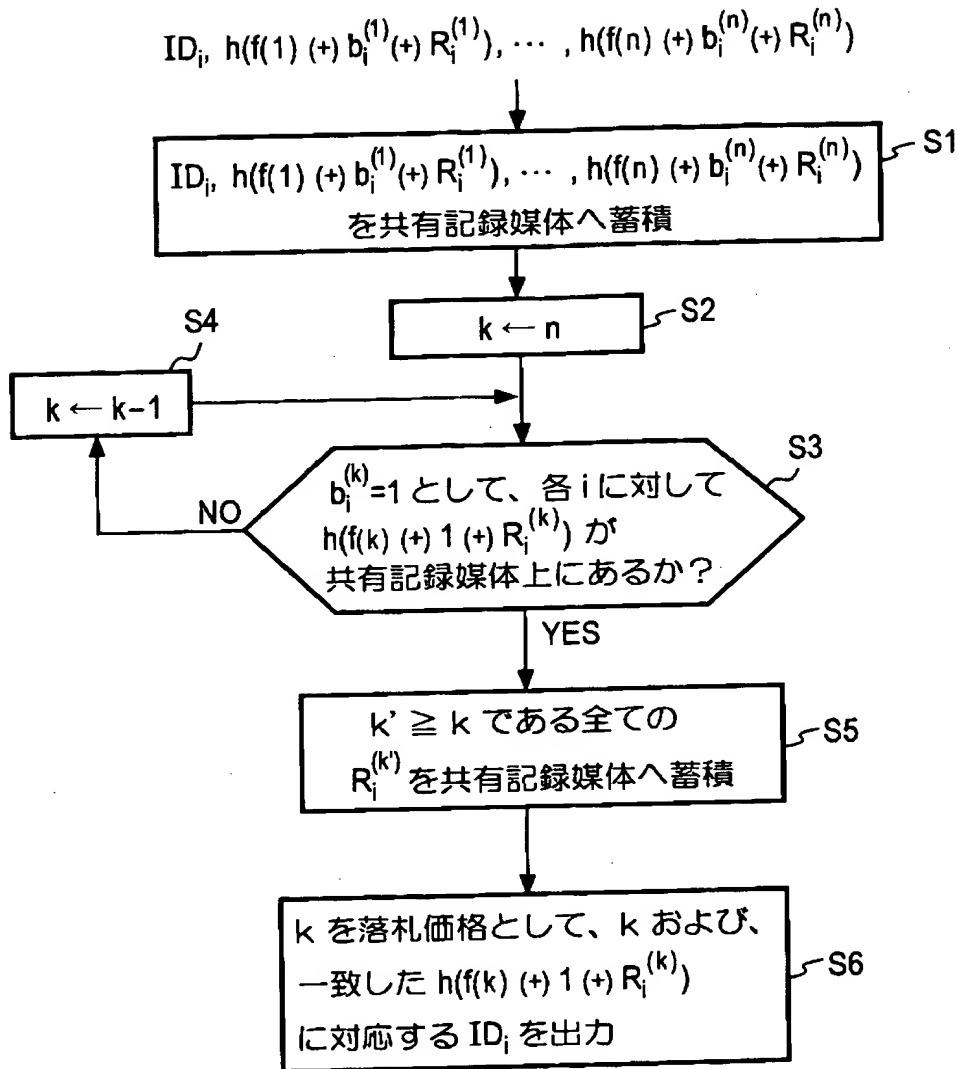
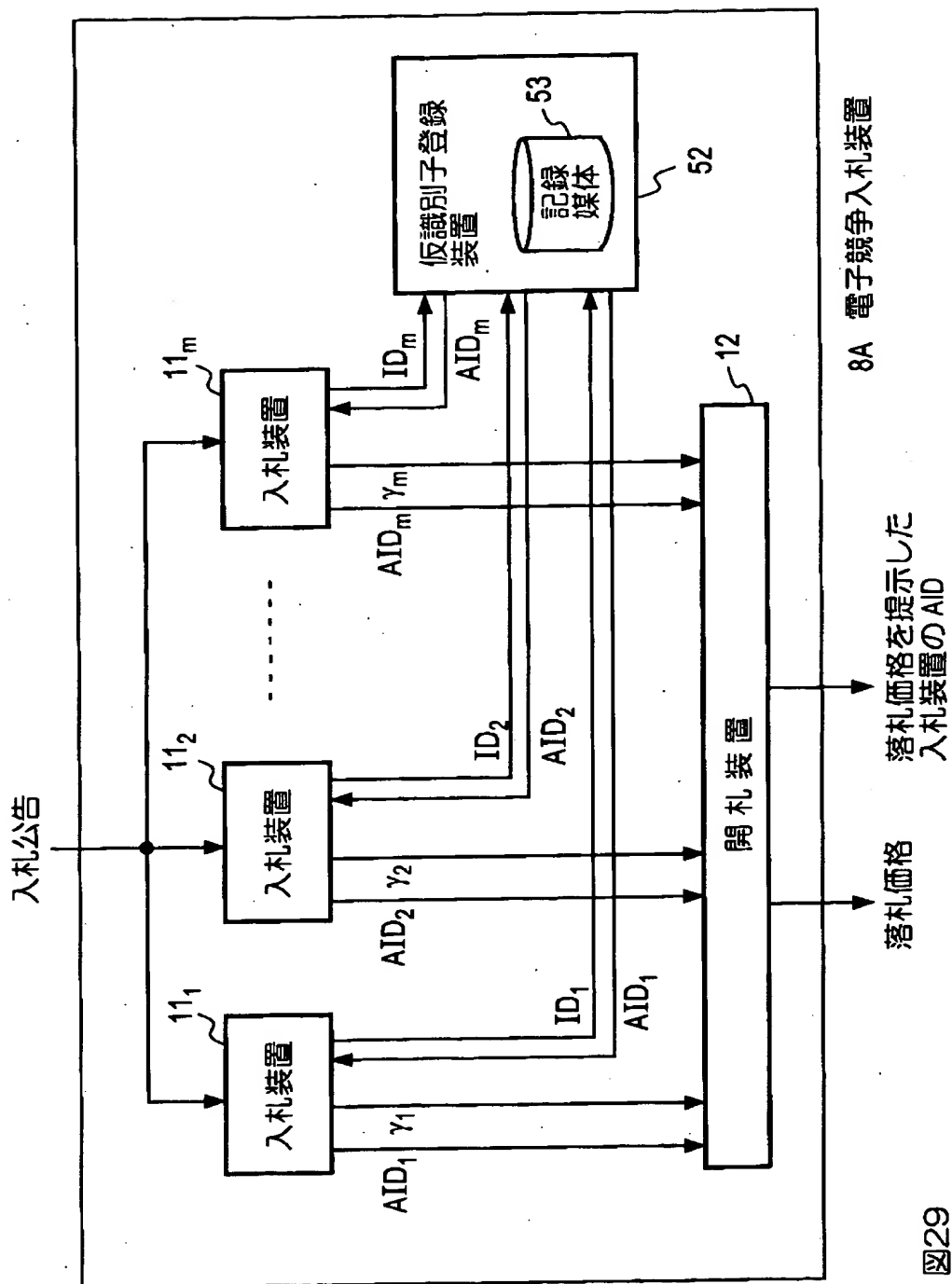


図28

【図 2 9】



8A 電子競争入札装置

図29

【図 3 0】

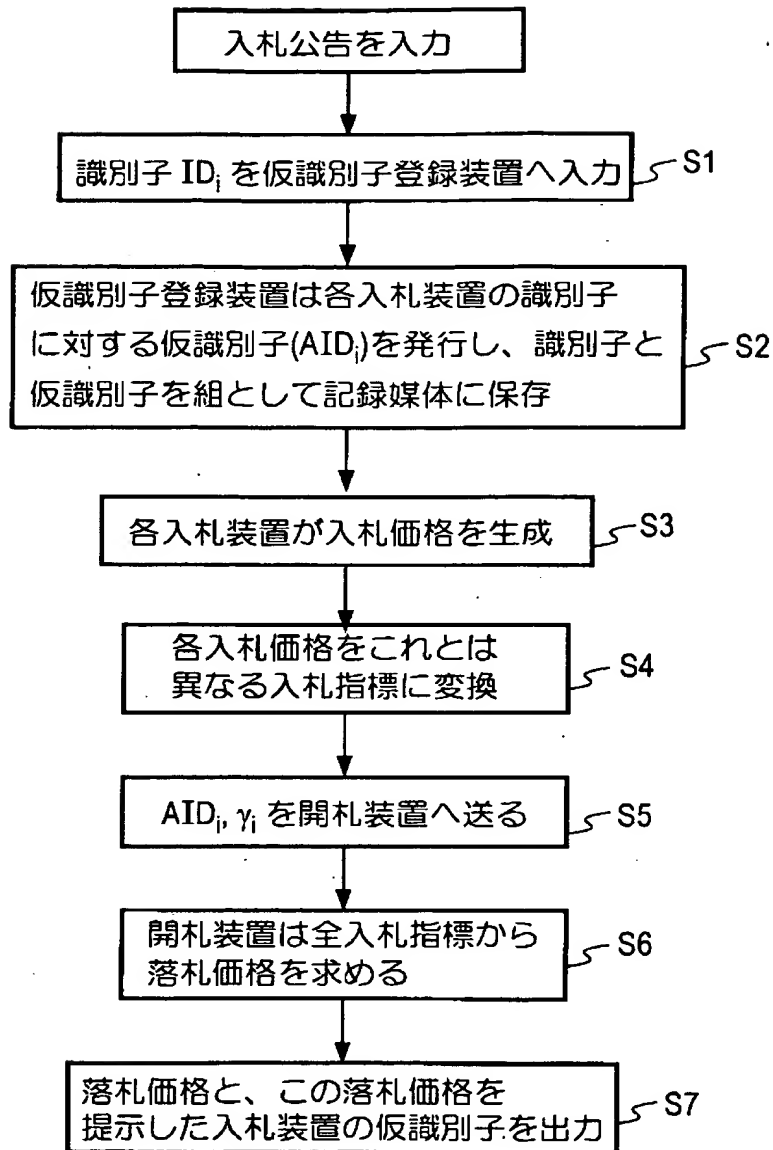


図30

【書類名】 要約書

【要約】

【課題】 入札価格 PR_i が他の入札装置から知られない。

【解決手段】 入札装置 11_i から入札指標 $r_i = g(h^{f(PR_i)}(IV_i))$ (IV_i は初期値、 $h^{f(PR_i)}$ はハッシュ関数 h を $f(PR_i)$ 回処理、 g ハッシュ関数) と入札装置 11_i の ID_i を入力し、共有の記録媒体 25 に蓄積し (S1)、 k を入札の上限値 n とし (S2)、 $i = 1$ とし (S4)、 $f(k)$ を生成し (S7)、 IV_i を初期値として $\delta_i = h^{f(k)}(IV_i)$ を生成し (S8)、 δ_i ($-g(\delta_i)$ を作る) (S9)、この δ_i と一致する r_i が記録媒体 25 にあるかを調べ (S10)、なければ、 i を +1 して、次々と、各入札装置について調べ、全入札装置の数 m について調べ終ると、 k を -1 して、同様にして $\delta_i = g(h^{f(k)}(IV_i))$ と一致する r_i があるかを調べ、一致した時の k を最高落札値とし、 k とその r_i の ID_i を出力する。

【選択図】 図 8

【書類名】 手続補正書

【整理番号】 NTTH115596

【提出日】 平成11年 7月22日

【あて先】 特許庁長官殿

【事件の表示】

 【出願番号】 平成11年特許願第205004号

【補正をする者】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

【代理人】

 【識別番号】 100066153

 【弁理士】

 【氏名又は名称】 草野 卓

 【電話番号】 03-3350-6456

【手続補正 1】

 【補正対象書類名】 図面

 【補正対象項目名】 図 7

 【補正方法】 変更

 【補正の内容】 1

【手続補正 2】

 【補正対象書類名】 図面

 【補正対象項目名】 図 1 0

 【補正方法】 変更

 【補正の内容】 2

【手続補正 3】

 【補正対象書類名】 図面

 【補正対象項目名】 図 1 2

 【補正方法】 変更

 【補正の内容】 3

【手続補正 4】

【補正対象書類名】	図面
【補正対象項目名】	図 1 4
【補正方法】	変更
【補正の内容】	4
【ブルーフの要否】	要

【図 7】

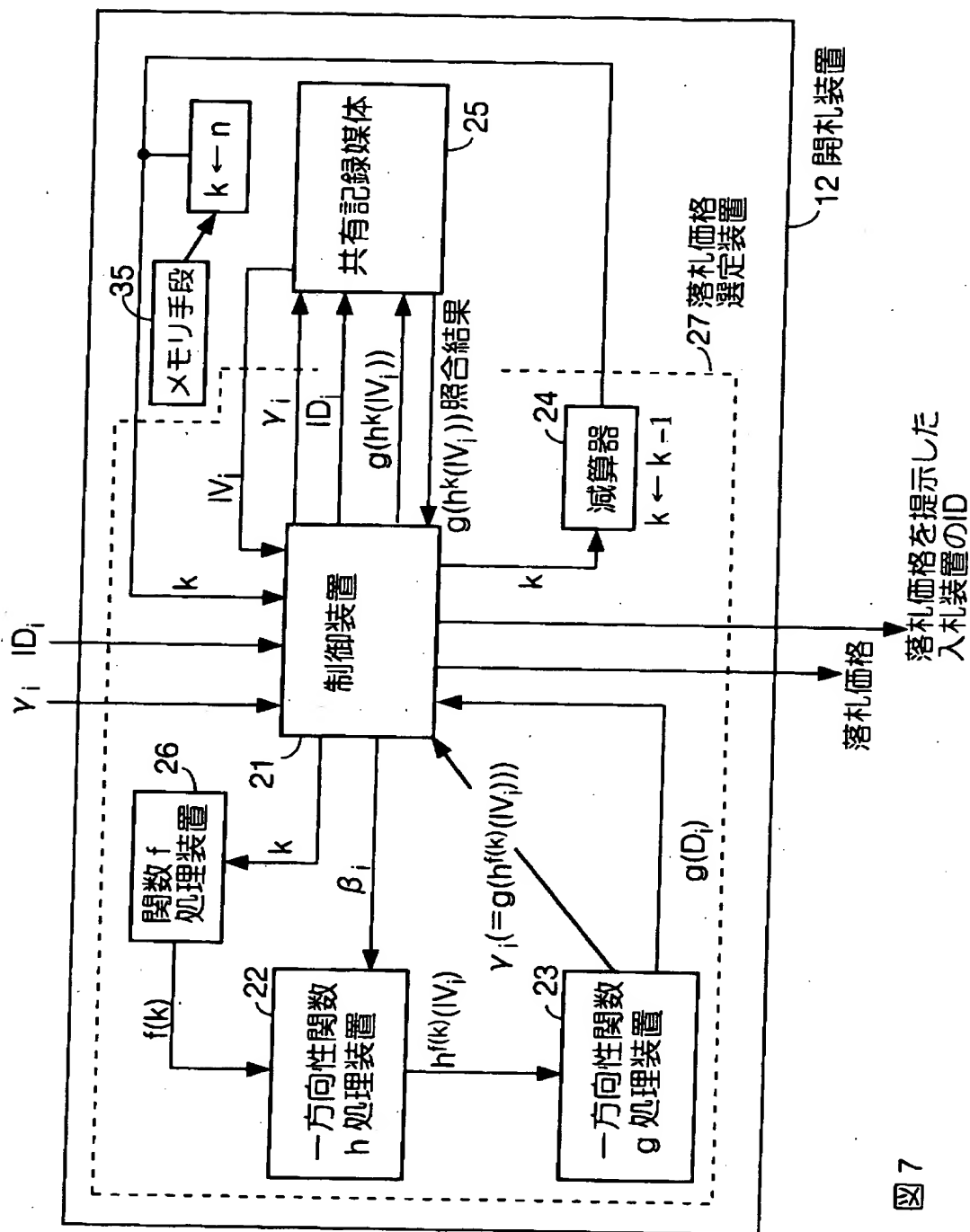


図 7

【図 1 0】

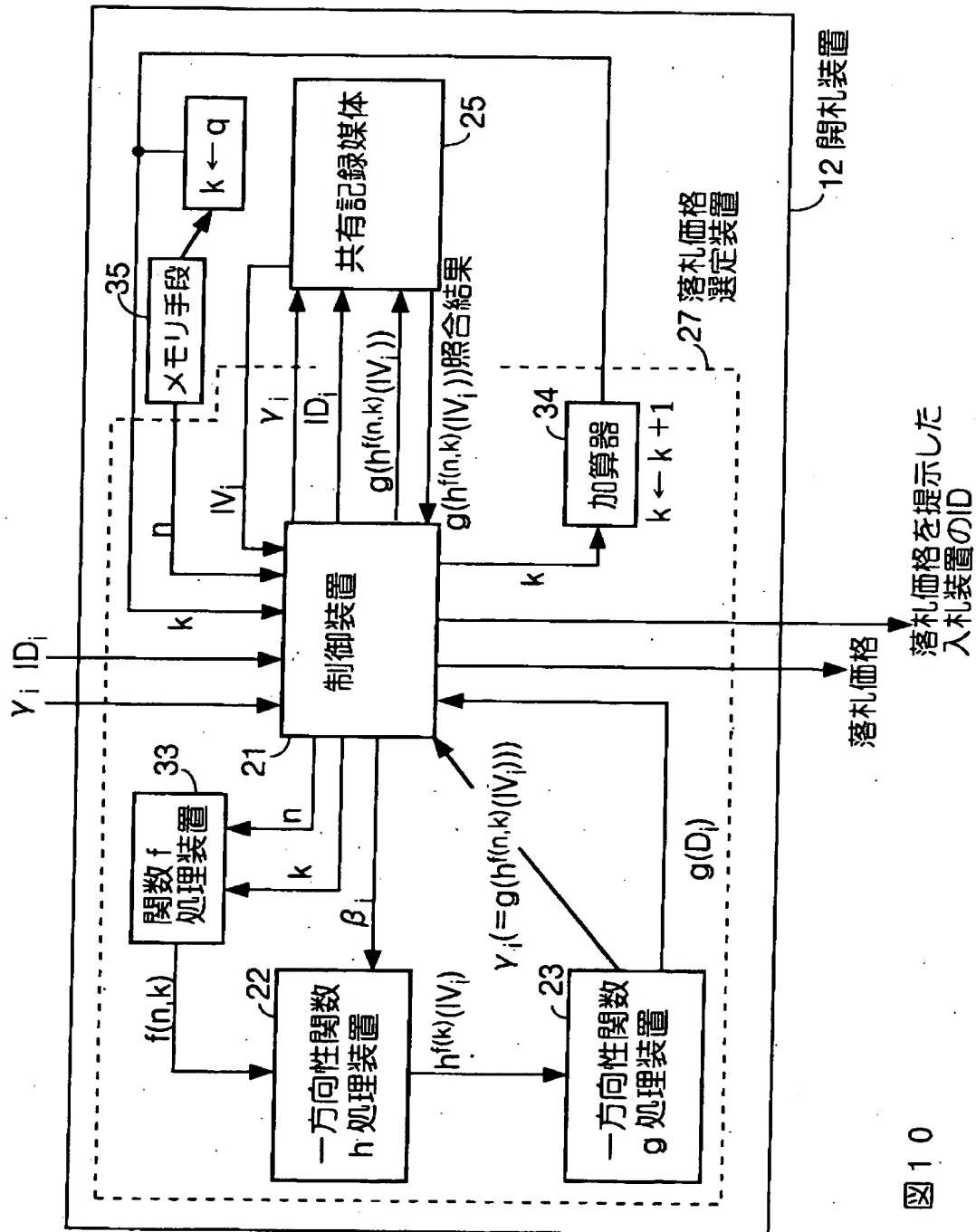


図 1 0

【図 12】

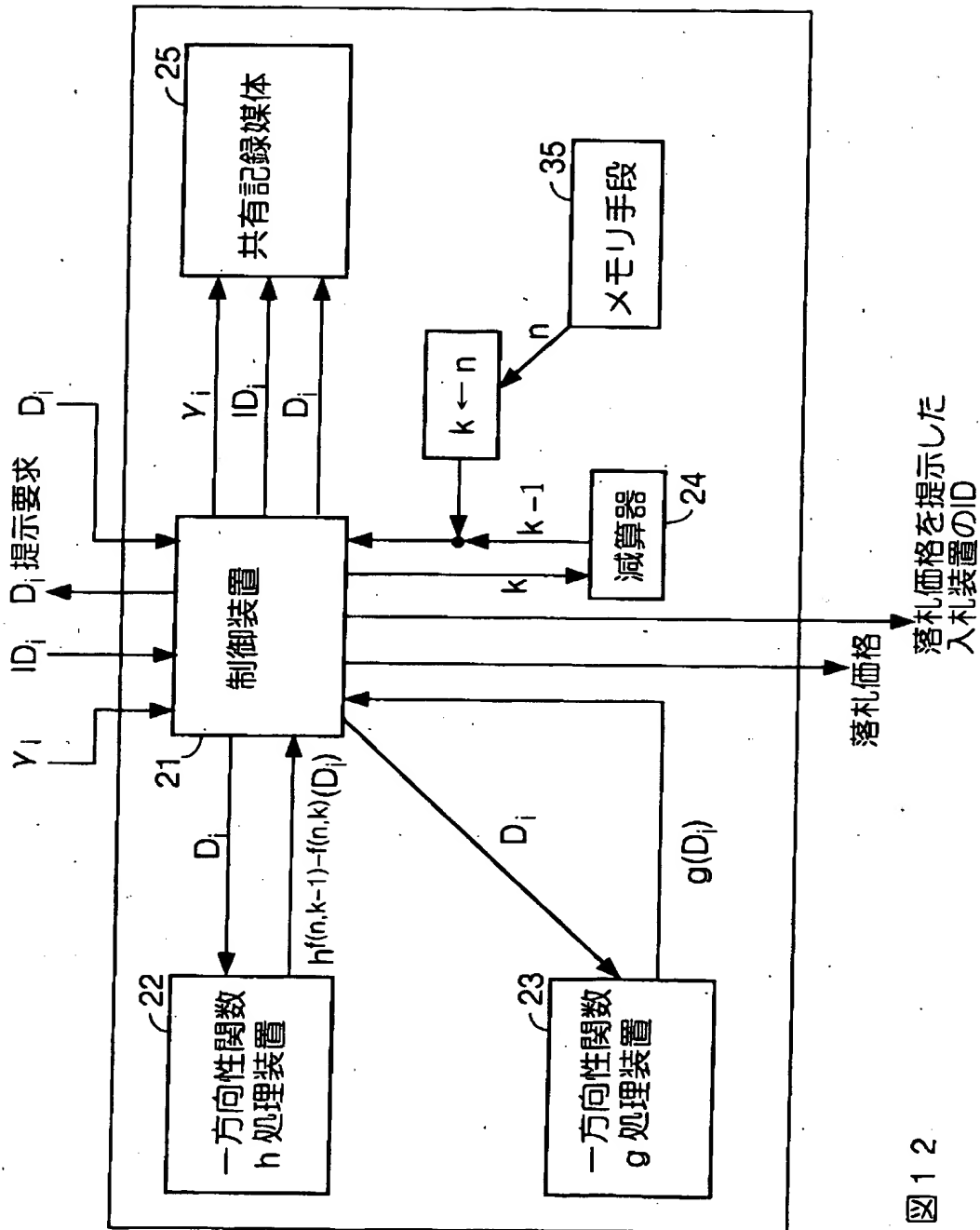


図 12

【 図 1 4 】

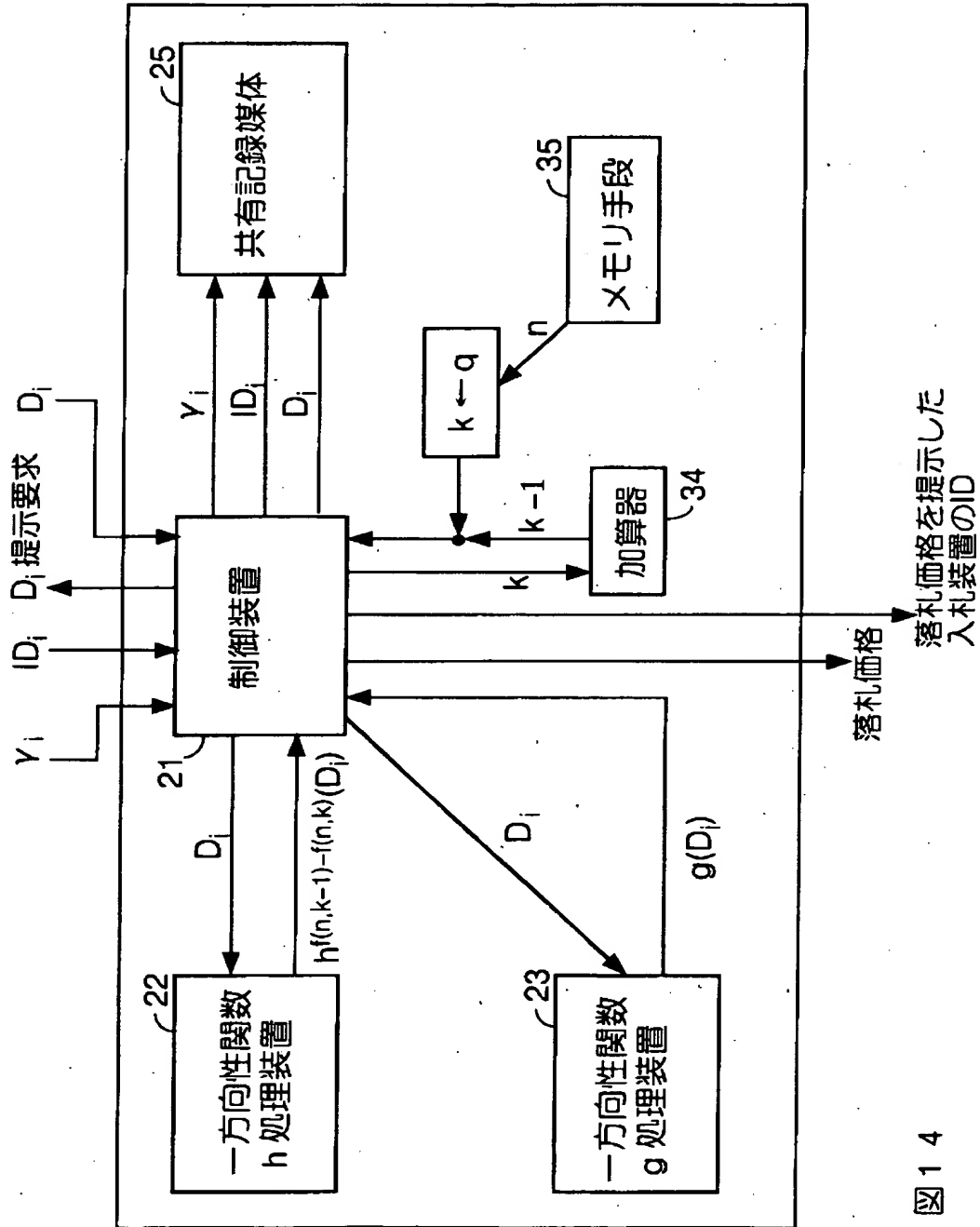


図 1 4

認定・付加情報

特許出願の番号	平成11年 特許願 第205004号
受付番号	59900702561
書類名	手続補正書
担当官	坪 政光 8844
作成日	平成11年 7月27日

<認定情報・付加情報>

【補正をする者】

【識別番号】	000004226
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名又は名称】	日本電信電話株式会社

【代理人】

申請人	
【識別番号】	100066153
【住所又は居所】	東京都新宿区新宿四丁目2番21号 相模ビル
【氏名又は名称】	草野 卓

出 願 人 履 歴 情 報

識別番号

[000004226]

1. 変更年月日 1999年 7月15日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目3番1号
氏 名 日本電信電話株式会社